2000

Smart Card Systems: Development of a Paradigm for a University-Wide Smart Card Student Identification System

Joanne M. Marlowe
Nova Southeastern University, drjomag59@gmail.com

Smart Card Systems: Development of a Paradigm for a University-Wide Smart Card Student Identification System

by

Joanne M. Marlowe

A Dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

School of Computer and Information Sciences
Nova Southeastern University

2000

We hereby certify that this dissertation, submitted by Joanne M. Marlowe, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Marlyn Littman — April 7, 2000

Marlyn Kemper Littman, Ph.D.
Chairperson of Dissertation Committee

Date

Trudy Abramson — April 7, 2000

Trudy Abramson Ed.D.
Dissertation Committee Member

Date

Sumitra Mukherjee — 4/10/2000

Sumitra Mukherjee, Ph.D.
Dissertation Committee Member

Date

Approved:

4-11-00

Edward Lieblein, Ph.D.
Dean, School of Computer and Information Sciences

Date

School of Computer and Information Sciences
Nova Southeastern University

2000

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Smart Cards: Development of a Paradigm for a University-Wide Smart Card Student Identification System

by
Joanne M. Marlowe

February 2000

College and university campuses present an ideal environment for smart card systems and offer one of the best opportunities for the early adoption of smart card technology in the United States. This study investigated the design, development, and implementation of a smart card system in the university environment, specifically Nova Southeastern University. Additionally, this dissertation investigation developed a paradigm for a university-wide smart card student identification system capable of providing multiple applications such as portable identity, secure access, and electronic purse function. This dissertation investigation employed a Modern Systems Development Life Cycle (MSDLC) methodology along with a case study strategy. Through case study analysis, in concert with an MSDLC methodology, this researcher determined how other colleges and universities implemented smart card systems and examined smart card capabilities and constraints.

The proposed model is based on an analysis of 23 colleges and universities currently utilizing smart card technology as part of their campus card systems. In this multiple-case study, the goal was to build a general paradigm that fits each of the individual cases, even though the cases varied in their details. This paradigm documents the development and implementation of a smart card system in a university environment.

As noted in this paradigm, the campus card combines magnetic strip and smart chip technology and is a managed card system. In addition, the campus card system includes strategic partnerships with merchants, banks and long distance carriers and is implemented in a phased process. The findings and conclusions of this dissertation inquiry can be generalized to other academic institutions investigating the viability of a smart card system.

It is important to note that this paradigm is based on an investigation of the small number of colleges currently utilizing smart card technology. However, this paradigm represents key considerations that should be addressed by academic institutions contemplating the installation of a multi-application smart card student identification system. The paradigm is subject to change as a consequence of innovations in the technological domain. Therefore, the smart card information system paradigm should be regularly reviewed and revised to reflect technological advancements.

Acknowledgments

I wish to acknowledge the many individuals who have given their time in support of this dissertation inquiry. Grateful appreciation is due my Dissertation advisor, Dr. Marlyn Kemper Littman for her invaluable advice, enthusiasm, and encouragement during the research process. Additionally, I would like to express sincere gratitude to my advisory committee members, Dr. Trudy Abramson and Dr. Sumitra Mukherjee, for their support and advice throughout this inquiry. Sincere thanks to Carole Ann Creque for her valuable input and assistance and to Christopher Ott for sharing valuable information. I would like to especially thank my parents, Charles and Patricia Saunders, for their sacrifices in affording me the opportunity to obtain a good, strong educational background and to God for enabling me to achieve it. Finally, I would be remiss if I did not acknowledge my sincere appreciation to my husband and mentor, Dr. Jamie Edsel Marlowe. It would be difficult to imagine this project gaining fruition without his endless inspiration, constructive criticisms, valuable contributions and, most importantly, his unselfish support and sacrifice. J. Edsel, I thank you for encouraging me to be all that I can be.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter I

Introduction

Statement of the Problem to Be Investigated and Goal to Be Achieved

A multiple application campus card was first introduced at Duke University in 1985 and employed magnetic strip technology operating in an on-line mode (Blackburn, 1993). The concept of one campus card for multiple applications continues to grow in popularity. Blackburn (1993) cites three principle factors for the movement to card system installations: (a) increased revenues derived from debit card sales, (b) increased concern for safety of person and property on college and university campuses, and (c) cost savings achieved through the use of a single card system.

According to White (1998), multi-application smart cards are the current trend on college and university campuses. Additionally, smart card technology is seen as a very new technology on college and university campuses (Campus ID Report, 1997). The National Association of Campus Card Users (NACCU) estimates that 25 of the country's 3,500 college campuses use smart cards, compared with approximately 1,250 that use magnetic strip technology (O'Sullivan, 1997). According to Smith, Cunningham and Cunningham (1997), the college and university market can serve as a microcosm for an examination and assessment of smart card functionality.

This dissertation inquiry investigates and focuses on the design, development, and implementation of a smart card system in the university environment, specifically, Nova Southeastern University (NSU). The goal of this study is to develop a paradigm for a university-wide smart card student identification system capable of providing multiple applications such as portable identity, secure access, class registration, secure email, and electronic purse functionality. A systems analysis and case study approach is used to conduct the inquiry.

Relevance and Significance

This dissertation investigation documents a paradigm for the development and implementation of a smart card system in a university environment. According to Wand and Thermos (1998), colleges and universities are installing state-of-the-art access-control systems that provide everything from entry to residence halls to the ability to make purchases off-campus. For example, the University of Pennsylvania utilizes smart cards to replace cash transactions both on and off campus. According to Wilen (1997), the PennCard's electronic purse function can be used to purchase books, tickets, copies, groceries, and, eventually, beverages in bars. This University issues the cards to increase convenience and university revenues and improve safety (Wilen, 1997).

This dissertation further describes the current and potential uses of smart cards on college and university campuses. Currently, students on more than 25 U.S. college campuses are using microchip-based smart cards to make telephone calls, launder clothes, purchase food and access grades.

In September, 1997, Guilford College became the first college in North Carolina to implement a campus-wide, fully integrated smart card program with a banking

component (CardTrak, 1997). The Guilford College smart card system is a fully functional one-card system that is used for college identification, library check-out, entry into security systems, and debit and vending programs on campus (CardTrak, 1997).

Florida State University (FSU) has implemented the FSUCard. Currently, however, the FSUCard serves only as an electronic purse to be used at drink and snack machines, photocopiers, microfiche copiers, laundry machines, and laser printers (FSU Card Services, 1996). Projected services include provision of secure intranet access to FSU records, ability to purchase books at the university bookstore, and connectivity to local and long distance telephone services.

Washington University in St. Louis has implemented the CacheCard. The CacheCard contains a microprocessor, or chip, with 8,000 bytes of memory as well as several magnetic strips (Washington University in St. Louis, 1998). The chip serves as an electronic purse for storing money in a student's account. The magnetic strips give the student access to certain campus services such as entry to campus housing and on-campus student activities, as well as meal points for use in campus dining areas.

Villanova University has implemented an all-purpose ID card called the Wildcard. The Wildcard combines smart card technology with magnetic strip technology to provide building access and electronic purse capabilities (Villanova University, 1998). The Wildcard's electronic purse can be used at selected off-campus merchants.

White (1998) estimates the cost for implementing a campus card system to be approximately $250,000 for 5,000 students; $500,000 for 10,000 students; and $750,000 to $1 million for 15,000+ students. According to White (1998), most universities phase

in the card system over a three to five year period. Smart card student identification systems enable the use of one card, instead of many, for all the functions of campus life.

According to Cobb (1998), smart cards are one of the top technologies of 1998 and 1999. Thomasson and Baldi (1997) suggest two reasons for this explosive popularity. According to these authors, sophisticated telecommunication and computing technologies support smart card multi-functionality. Further, the smart card industry now has a defined technical and commercial smart card infrastructure that is still evolving. This infrastructure includes products and software as well as international security standards.

Intelligent smart cards contain a central processing unit (CPU) and feature the ability to store and secure information and execute the specific program required by the card issuer's applications needs (Smart Card Forum, 1998). Intelligent smart cards offer a read/write capability so that new information can be added and processed. For example, monetary value can be added and subtracted in accordance with the requirements of a particular application.

The significant characteristic of a smart card is its ability to process and interpret data. Farrell (1996) suggests that this ability to store and manipulate information means that smart cards can be used in a wide variety of applications. Additionally, recent technical advances such as increased memory capabilities and faster processor speeds along with standardization initiatives to address interoperability of cards, readers, and applications contribute to multi-functional smart cards that perform more than one function. Florida State University, University of Central Florida, and Villanova

University are implementing multifunctional, multipurpose access cards that serve as library cards, electronic purses, and parking permits for faculty, students, and staff.

Smart cards exhibit major technological advantages in comparison to conventional magnetic strip cards, memory cards, and bar coding. Magnetic strip cards carry information outside of the card on a magnetic strip that can be easily damaged or copied. As noted by Dreifus and Monk (1998), smart cards afford a higher level of security than magnetic strip cards and memory cards. The smart card's integrated circuit chip protects the stored information and makes it less vulnerable to damage and/or theft. This higher level of security makes smart cards viable in monetary transactions and applications involving proprietary secrets and personal data (Fancher, 1997).

Smart card technology continues to evolve. Further advances in technology may mean that consumers will not have to carry multiple smart cards. Rather, they will utilize one card for several applications. According to Farrell (1996), smart cards can carry up to 100 times more information than a magnetic strip card and hold this information more reliably. With its high memory capacity, a smart card is capable of running multiple applications on one card at a cost comparable to today's single-application cards (Chips: Smart cards get smarter, 1998).

Barriers and Issues

A smart card can be simplistically defined as a credit card with brains. Typically equipped with an 8-bit microcontroller that has the computing power of the original IBM personal computer, a smart card is the same size and shape as a magnetic strip card (Guthery & Jurgensen, 1998).

Data storage capabilities of smart cards exceed those of magnetic strip cards. However, the capabilities of the smart card must be balanced against the application needs of a university campus setting (Printup, 1997).

In 1993, Loyola College located in Baltimore, Maryland represented the only multiple application smart card site in the United States (Blackburn, 1993). In the early 1990s, smart cards enjoyed limited success and had minimal campus visibility (Blackburn, 1993).

Today, smart cards still enjoy limited success on college and university campuses. Due to steep implementation costs, approximately two dozen of the more than 3,000 colleges and universities have installed smart card systems (Card Technology, 1999). Examples include the University of Arizona and Penn State University. These universities utilize only one smart card-based application in conjunction with magnetic strip technology.

There are several reasons for the limited success of smart cards. Smart cards are significantly more expensive to implement than magnetic card technology. According to *Global Smart Card Opportunities*, a 1998 report published by the London-based researcher Datamonitor, smart cards and smart card terminals cost up to seven times more to manufacture than magnetic strip cards and magnetic card readers (Craig, 1998). Additionally, administrative costs are also higher. Start-up costs and implementation costs present an almost insurmountable obstruction to installing a smart card system (Craig, 1998).

According to Tom and Driver (1998), the cost of upgrading point of sale (POS) terminals with smart card technology averages $500 per terminal. The cost of upgrading

ATM machines to offer smart card compatible banking services is approximately $3,000 per machine (Tom & Driver, 1998). Importantly, Craig (1998) reports that according to Summit Research Associates in Rockville, Maryland, smart card costs have dropped substantially. Further, Craig (1998) predicts costs will continue to fall once industry standards are in place.

Smart card replacement costs are also significantly more expensive than magnetic strip cards. The projected cost for smart card distribution is estimated at $2 to $10 per card compared to approximately $.50 per magnetic strip card (Printup, 1997, Tom & Driver, 1998).

Thomasson and Baldi (1997) state that, at present, the smart card market is still mainly European. Smart cards are found in a variety of configurations. These cards are currently used in the financial industry for e-cash applications, healthcare insurance industry to track medical claims, and transportation industry for ticketless airline and toll road payments. Today, there are over 100 million pay-phone cards in France and 80 million health insurance cards in Germany based on smart card technology. Electronic purse cards are in use in more than 20 countries (Cobb, 1998).

Smart cards are deployed worldwide for electronic identification applications. Driver's licenses, passports, and identification cards combine smart card and photo identification technologies (Dreifus & Monk, 1998). Examples include smart driver's license programs in Argentina and China. These initiatives are discussed in Chapter 2.

The implementation of smart card applications has lagged in the United States. Explanations for this range from the success of magnetic strip cards to privacy concerns and religious opposition (Cobb, 1998). Additionally, most of the smart cards in use

today are single application cards. According to Fancher (1997), smart cards must handle several applications before gaining widespread acceptance in the United States.

American attitudes toward electronic money are also impeding smart card implementations. According to Dreifus and Monk (1998), many Americans are reluctant to handle money electronically. The 1996 Atlanta Olympics introduced the first stored-value smart card program in the United States called the Visa Cash card. This card was a single-application electronic purse designed to be discarded after all the value was depleted (Dreifus & Monk, 1998). However, not all merchants could be convinced to accept the card. Additionally, consumers became confused since the Visa Cash card was different from a standard Visa credit card. Visa failed to properly educate consumers and convince merchants to accept the Visa Cash card (Dreifus & Monk, 1998). As a consequence, this program was a failure.

However, according to Thomasson and Baldi (1997), magnetic strip cards will gradually be replaced with smart cards. Current estimates suggest an average smart card growth rate of 47% over the next five to six years (Thomasson & Baldi, 1997). This growth is attributed to advances in technology and in the overall system architecture.

According to Farrell (1996), advancements in semiconductor technology can contribute to development of a smart card microcontroller chip that is smaller, cheaper and more versatile, and offers a wider range of features. The success of smart cards hinges on two key factors. These are compatibility and standardization within the smart card industry and acceptance by merchants and consumers.

Compatibility and Standardization

Although smart card technology has been in existence for over 20 years, the lack of standards impede adoption (Kosiur, 1997). According to Basch (1998), the majority of smart card systems deployed worldwide utilize proprietary operating systems and incompatible standards. For example, a prepaid American phone card may not function in a Canadian pay telephone.

Smart card applications are specifically tied to the card's operating system. The operating system, in turn, is tied to a specific chip. As a consequence, a user may carry a different smart card for each application. According to Watson (1997), the lack of compatibility between smart cards is a hindrance to their adoption by consumers and merchants.

Industry experts such as O'Sullivan (1999) agree that interoperability is an important and contentious issue impacting smart card deployment. Vendors have developed applications that run on proprietary operating systems that are incompatible. Stored value applications, or e-purses, are associated with specific operating systems. For example, Mondex is associated with MULTOS, the Multi-Application Operating System developed by a consortia led by MasterCard (O'Sullivan, 1999). Visa Cash is associated with the Java Card, also called the Open Card Framework (O'Sullivan, 1999). According to O'Sullivan, (1999) there is also an emerging e-purse application that combines elements of the Java Card with elements of Proton, the most common e-purse in Europe. These proprietary applications further delay multi-application smart cards that appeal to consumers. Chapter 2 discusses in detail the efforts currently underway to promote standardization and compatibility within the smart card industry.

User Acceptance

Visa, MasterCard, Chase Manhattan Bank, and Citibank conducted a 14-month pilot project in which approximately 100,000 smart cards were issued to New York's Upper West Side residents for use at more than 600 local stores in 1997 and 1998 (Alcorn, 1998). The cards were designed to replace cash. Users loaded value from their private bank accounts onto their smart cards and then used these cards to pay for routine items and services such as groceries, video rentals, and dry cleaning. Two-thirds of the merchants originally committed to participate in the project prematurely ended their participation because consumer usage was insufficient (Alcorn, 1998). Reasons given for the project's failure were varied and included the following: 1) consumers did not know how to use the system; 2) salespeople did not know how to process transactions; and 3) many of the West Side residents commuted to work in other parts of New York where the cards could not be used.

Merchant Acceptance

Shanahan, whose firm Shanahan & Associates researched the smart card pilot program at the 1996 Summer Olympics, found the hurdles hindering smart card success to be more psychological than technological (O'Sullivan, 1999). According to Shanahan, the biggest barrier centered around merchant acceptance.

Future of Smart Cards

In 1996, the smart card market increased by an estimated 100%, including a growth of approximately 700% in banking applications (Berinato & Kerstetter, 1998). Berinato and Kerstetter (1998) suggest that smart cards are gaining support from PC

(personal computer) makers and vendors in response to increased demand for enterprise and network security.

Smart cards are an effective way of ensuring secure access to open interactive systems. These cards support diverse functions that include encryption key mobility, secure single sign-ons, and electronic digital signatures. Expectations are that explosive growth in smart card deployment in the United States will be led by security-specific applications such as email encryption on personal computers and user authentication on network computers.

According to Thomasson and Baldi (1997), the smart card industry is creating a comprehensive technical and commercial infrastructure. This infrastructure supports participation by software suppliers, subcontractors, and standards organizations; features high level commercial cooperation; and promotes collaboration and development of international security standards.

The smart card industry continues to mature and it is not unrealistic to imagine that appliances ranging from televisions to refrigerators will be equipped with smart card readers within the next 3 to 5 years. According to Dreifus and Monk (1998), the greatest growth in card-equipped appliances will be on college and university campuses where smart cards can routinely provide access to vending machines, television sets, washers, and dryers.

Purpose of the Research Investigation

This investigation examines smart card capabilities in terms of Nova Southeastern University's (NSU's) mission, goals, objectives and requirements. Factors impacting

smart card design and development are examined. A paradigm for smart card implementation will be developed.

The specific purposes of this dissertation investigation are to:

- Review relevant literature on smart cards and smart card systems implementation;
- Determine how other universities and colleges have implemented a smart card system;
- Determine the benefits and limitations of smart cards in higher education; and
- Develop a paradigm for the development and implementation of smart card systems in higher education based on the NSU case study.

The findings and conclusions of this dissertation investigation can be generalized to other academic institutions investigating the viability of a smart card system.

Limitations and Delimitations of the Study

This dissertation investigation is somewhat limited by the small number of colleges and universities currently utilizing single-application and multi-application smart card systems. However, since all of the participants are utilizing smart cards in a similar manner (electronic purse, library card, access), it is assumed that these colleges and universities are representative of the broader population of higher education institutions. Therefore, it is assumed that the findings of this dissertation investigation will be appropriate for other colleges and universities implementing smart card systems.

Definition of Terms

CPU. Central processing unit. The integrated circuitry that executes the program stored on a smart card (Guthery & Jurgensen, 1998).

EEPROM. Electrically erasable, programmable ROM. Memory in a smart card that holds its contents when the power is removed. EEPROM is used to store smart card values that are set during personalization, such as account numbers or values. Values such as the amount of value stored on the card can change (Guthery & Jurgensen, 1998).

Electronic purse. A smart card that stores a small amount of money. Some electronic purses can be reloaded. Some must be discarded when they are financially depleted. Also known as E-purse (Guthery & Jurgensen, 1998).

FeRAM. Ferroelectric Random Access Memory. FeRAM is a nonvolatile technique that speeds memory access to as much as 20 times faster than EEPROM technology (Hofland & Janowski, 1998).

Java card. A smart card that contains a Java interpreter in its operating system. A Java smart card executes Java byte code (McGraw & Felten, 1999).

Magnetic strip card. A plastic card that contains a magnetic strip on the rear surface. The magnetic stripe is divided into three tracks that magnetically store data (Guthery & Jurgensen, 1998).

Memory card. A plastic card that contains a simple memory chip with read and write capability. Memory cards are designed for storing information or values and are commonly used for applications such as disposable prepaid telephone cards (Dreifus & Monk, 1998).

Microcontroller cards. True smart cards that contain a microprocessor unit, RAM, ROM, mass storage, input/output hardware, and an operating system (Dreifus & Monk, 1998).

RAM. Random access memory. Volatile memory that is used for temporary storage of data by the central processing unit data (Guthery & Jurgensen, 1998).

ROM. Read-only memory. Permanent memory that cannot be upgraded or changed. ROM usually contains the operating system of the smart card data (Guthery & Jurgensen, 1998).

Smart card. A piece of plastic the size of a credit card that contains a microprocessor chip. The chip provides secure access to the memory of the card and also may perform data-processing and communication functions data (Guthery & Jurgensen, 1998).

Summary

This chapter presents a rationale and foundation for conducting an investigation of smart card systems and their utilization in college and university environments. This dissertation inquiry includes an examination of processes leading to the design, development, and implementation of a smart card system at Nova Southeastern University and documents development of a paradigm for a university-wide smart card student identification system.

A case study analysis approach provides a framework for examining how other colleges and universities implement smart card systems and the benefits and limitations associated with these systems. Findings from this dissertation inquiry can be generalized to other academic institutions investigating the viability of a smart card system.

Chapter II

Review of the Literature

Overview

This chapter presents the review of related literature for this dissertation investigation. The literature reviewed in this chapter includes an historical overview, a presentation of smart card technical fundamentals, and a discussion on smart card standards and standards organizations.

An in-depth examination on the use of smart cards, both internationally and domestically, is also presented. To understand the potential use of smart cards, one must examine the plethora of functions currently dependent on smart cards. This chapter, therefore, also examines the use of smart cards in electronic commerce, telecommunications, travel and transportation, identification, healthcare, government, and education.

Although the growth of smart cards in the United States has been slow, the cards are gathering support from government agencies such as the National Security Agency, General Services Administration and the Department of Defense. Smart cards are also increasingly used on university campuses and in business (Nelson, 1998). Dreifus and Monk (1998) believe that this market growth can be attributed to the acceptance of smart cards by different industries, declining costs of smart cards, and the use of smart cards in emerging electronic commerce systems.

Brief History of the Smart Card

Smart card technology has been in existence for more than three decades. The first smart card patents were filed in February 1969 by two German engineers, Jurgen Dethloff and Helmut Grottrupp (Guthery & Jurgensen, 1998). One year later, Kunitaka Arimura of the Arimura Technology Institute in Japan filed for a smart card patent (Townend, 1999). In May, 1971, Paul Castrucci of IBM filed for and received an American patent entitled Information Card (Guthery & Jurgensen, 1998). However, the term smart card was not used until 1980 when it was coined by Roy Bright, a French publicist (Guthery & Jurgensen, 1998).

Roland Moreno is credited with launching the smart card industry as it is known today. Moreno, a French journalist, filed 47 smart card-related patent applications in 11 countries and founded the French company Innovatron (Guthery & Jurgensen, 1998). Moreno's patents were instrumental in launching both the memory chip-equipped cards, known as memory cards, and the microcontroller-based cards known as smart cards (Doheny, 1997). Moreno demonstrated the capability of installing integrated circuits on a piece of plastic the size of a credit card and launched the chip card industry.

Moreno's early chip-equipped cards were known as memory cards. Early memory cards were based on EEPROM (electrically erasable programmable read-only memory) and featured fixed digital circuits (Doheny, 1997). The early applications of memory cards included healthcare identification cards and telephone payment cards.

Smart cards are more secure than magnetic strip cards and were first adopted by the French banking association to combat credit card fraud. Motorola Semiconductor,

working with the French computer company Bull HN Information Systems designed the first smart card microchip for the French banking industry (Flohr, 1998). According to Flohr (1998), the first real smart card was a two-chip microcontroller-based card. Subsequently, Motorola unveiled a single-chip microcontroller-based smart card (Doheny, 1997).

Since 1988, with the smart card infrastructure in place, the French banking association witnessed a tenfold drop in credit card fraud (Doheny, 1997, Bull and Cartes Bancaires salute 10 years, 1999). In 1998, the fraud rate was reported to be 0.018%, down from 0.18% in 1988 (Bull and Cartes Bancaires salute 10 years, 1999). During this same period, the number of transactions nearly tripled, from 1.2 billion in 1988 to 3.1 billion in 1998 (Bull and Cartes Bancaires salute 10 years, 1999).

Credit cards store information on magnetic strips that are carried on the outside of the card and can be easily read and copied onto counterfeit cards. In comparison, the integrated circuit on the smart card protects the stored information and makes it less vulnerable to damage and/or theft. Smart card technology can also encrypt information and store it in areas that are designed to be unreadable.

Smart Card Technology Fundamentals

Overview

At its most basic level, a smart card consists of four components. These are the semiconductor, module package, software, and card. Other material on the card include printing, embossing, magnetic striping, personalizations, and holograms (Doheny, 1997). Today's chip cards exchange information through contact with a reader and are either memory or microcontroller-based. New combination smart cards include miniaturized

radio modems for sending and receiving data via a radio frequency (RF) transmission (Doheny, 1997).

A complete smart card consists of a central processing unit (CPU), read-only memory (ROM), nonvolatile read/write memory (EEPROM), temporary working memory (RAM), and an optional crypto-coprocessor (Cobb, 1998). Similar to computer hard drives and floppy disks, smart cards have their own file systems. According to Cobb (1998), an IBM multifunction card includes a master file (the root directory), dedicated files (application directories), and elementary files (the actual application data).

The most distinguishing element of the smart card is the semiconductor, or microchip. The microchip enables the smart card to process information as opposed to only storing and recalling information.

Smart Card Operating System

The smart card's software is installed at time of manufacture and consists of the card operating system (COS) (Doheny, 1997). Once the card operating system is burned into the ROM area of the microchip, the operating system is unalterable (Dreifus & Monk, 1998).

These operating systems resemble pre-DOS collections of on-card commands to which the smart card responds (Guthery & Jurgensen, 1998). In terms of operations, the terminal sends a command to the smart card. Subsequently, the smart card executes the command, returns the result to the terminal, and waits for another command. This basic relationship between the smart card terminal and smart card is one of master and slave (Guthery & Jurgensen, 1998).

Smart card operating systems support the classic set of file operations such as create, delete, read, write and update (Guthery & Jurgensen, 1998). Additionally, the specific operating system determines the operations the card is authorized to perform. Because there are limited card operating systems available, the choice of one over the other may dictate the microchip manufacturer, security capability and the card acceptance device (CAD) required for the proposed application (Dreifus & Monk, 1998).

Smart Card Communications

The communications channel in a smart card transaction is half-duplex. Data are transmitted in one direction, either from the smart card reader to the smart card or from the smart card to the smart card reader. Data cannot travel in both directions simultaneously.

A standard single-chip smart card is able to transmit and receive data at speeds up to 115,200 bits per second (bps) (Guthery & Jurgensen, 1998). However, most contact smart card terminals drive smart cards at 9,600 bps or 7,800 bps for contactless smart cards (Guthery & Jurgensen, 1998). Data are transmitted in small packets of 10 to 100 byte messages and stored in a buffer in the smart card's limited random access memory (RAM) (Guthery & Jurgensen, 1998). According to Guthery and Jurgensen (1998), ISO (International Standards Organization) and CEN (European Committee for Standardization) describe in detail the format and coding of messages. Optionally, smart card programmers can design messages to specifically fit his or her applications.

A transaction between the smart card and the card terminal involves six steps (Overview of smart card technology, 1999). These steps include:

- Activation of the contacts by the smart card reader;

- Resetting of the card by the reader;
- Answer-to-reset by the card;
- Optional selection of protocol type;
- Processing of successive commands; and
- Deactivation of the contact by the card reader.

Smart Card Memory System

A smart card contains three types of memory (Guthery & Jurgensen, 1998). These are read-only memory (ROM), nonvolatile memory (EEPROM), and random access memory (RAM). Figure 1 illustrates the typical layout of a chip and the amount of space required for each of the different types of storage and processing elements.

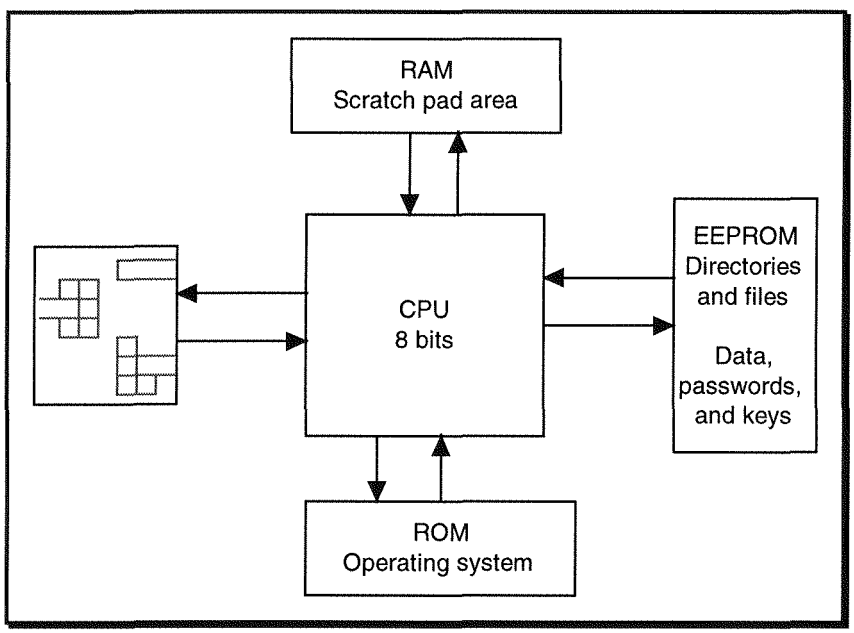


Figure 1. Chip Card Physical Layout.
Note. From *Smart Cards: A Guide to Building and Managing Smart Card Applications* (p. 107), by Henry Dreifus and J. Thomas Monk, 1998, New York, NY: John Wiley & Sons, Inc.

The largest area on a per-bit basis is the RAM, followed by the EEPROM. The smallest area of memory is the ROM (Dreifus & Monk, 1998).

The smart card operating system is stored in the ROM along with any code and data. ROM is programmed during manufacture and is unchangeable. Most smart cards have between 8 KB and 32 KB (kilobits) of ROM, although ROM sizes are increasing to meet the more complex programs that are emerging in the industry (Guthery & Jurgensen, 1998, Dreifus & Monk, 1998).

Nonvolatile memory (NVM), or EEPROM, stores the card's variable data such as account numbers, amount of e-cash or loyalty points. Nonvolatile memory can be read or written by applications programs and retains its contents when power is removed from the card (Guthery & Jurgensen, 1998). NVM range from 1 KB to 16 KB and are considered a precious resource on the smart card. Each file in NVM takes up some extra administrative bytes in addition to the bytes actually in use (Guthery & Jurgensen, 1998). The administrative, or overhead, bytes describe the file format including file size and type as well as access conditions. According to Dreifus and Monk (1998), the size of NVM affects the format, capabilities, and price of the microchip.

According to Guthery and Jurgensen (1998), RAM is also considered a precious resource on the smart card. Smart cards contain 1,000 bytes or less of RAM. This small amount of memory often becomes a constraint when designing smart card programs (Dreifus & Monk, 1998). For example, the software developer must be aware of the amount of RAM that will be utilized by a specific application. Additionally, Guthery and Jurgensen (1998) state that RAM is not only used by the programmer's application but also by all utility routines.

Intelligent Smart Cards Versus Memory Cards

There are two basic kinds of smart cards, specifically, intelligent smart cards and memory cards. Intelligent smart cards contain a central processing unit (CPU). They store and secure information and execute decisions as required by the card issuer's specific applications needs (Smart Card Forum, 1998). Intelligent smart cards offer a read/write capability, so that new information can be added, deleted, or modified and then processed. For example, monetary value can be added or deleted as a particular application requires.

Memory cards are primarily information storage cards. The card contains stored values that the user can spend at a pay phone, retail store, or vending area. Memory cards are not considered true smart cards because they cannot process information or provide for multiple application capabilities (Flohr, 1998).

Contact Versus Contactless Smart Cards

The information contained in a smart card is processed in two ways. Contact cards exchange data through a reader. Contactless cards transmit data without contact via a built-in miniaturized radio modem (Flohr, 1998). Contact cards must be inserted into a terminal to transmit information. Contactless cards integrate radio frequency (RF) technology to enable auto-teller transactions without the need for inserting the card into a reader (MacLellan, 1997).

Next Generation Smart Cards

Traditional smart card microprocessors typically allow 64 KB of 8-bit memory (Hofland & Janowski, 1998). Advanced cryptography and more sophisticated operating systems require additional memory resources. Next generation smart cards are expected

to utilize 32-bit processors for enabling applications to operate up to 60 times faster than on the existing 8-bit processor cards (Hofland & Janowski, 1998).

Additionally, the industry is currently moving to replace EEPROM memory technology with ferroelectric RAM (FeRAM) to further improve smart card functionality. FeRAM is a non-volatile memory that does not lose its data in the event of a power shut-off (Hyundai, 1998). Motorola and Matsushita have worked on the development of FeRAM since 1993 (Hofland & Janowski, 1998). In April 1996, Matsushita and Motorola introduced the first commercial use of fatigue-free, non-volatile memory in a read/write radio frequency identification smart card (Symetrix, 1998).

In mid-1998, NEC Corporation introduced an embedded ferro-electric random access memory (FeRAM) for smart cards that is 10,000 times faster and consumes 10,000 times less energy than previous EEPROM devices (NEC, 1998). According to Hofland and Janowski (1998), FeRAM is a nonvolatile technique that speeds memory access to as much as 20 times faster than EEPROM technology.

FeRAM significantly improves the memory's write-speed and its energy savings compared to conventional EEPROM. Additionally, FeRAM offers higher security benefits for smart card microcontrollers and enables smart cards to be powered only by energy in electronic waves (NEC, 1998).

These increases in processing power and memory, as well as the use of higher level programming languages such as Java, allow FeRAM-enabled smart cards to perform complex mathematical functions as well as multiple applications. This processing power is not possible with traditional 8-bit processor cores.

Recent advances in technology such as Card Java, increased processor speeds, and standardization initiatives may also mean that consumers will not have to carry multiple smart cards, but can utilize one card for several applications. This high memory capacity enables card issuers to run multiple applications on one card at a cost comparable to today's single-application cards (Chips: Smart cards get smarter, 1998).

With smart cards getting smarter, security features become indispensable. Motorola has recently developed a special shield for preventing external visual examination, as well as a superior memory-partitioning capability for making each application secure and distinct. With these technical advances, moreover, multiple applications on a chip become viable (Chips: Smart cards get smarter, 1998).

Smart Card Standards and Standards Organizations

Since the early 1980s, the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), the European Committee for Standardization (CEN), the European Telecommunications Standards Institute (ETSI), and the British Standards Institute (BSI) have aggressively worked to identify the interoperable ways in which smart cards can be defined for international use (Dreifus & Monk, 1998).

Standards specify the characteristics of credit cards, telephone cards, and smart cards. As a general rule, standards are not mandatory, but are voluntary. Additionally, standards reflect the results of joint work and are validated by consensus to represent all relevant interests (World Standards Services Network, 1998).

International Standards

International technical standards are protected by the copyright of the international standards body which is composed of the International Organization for Standardization (IOS) and the International Electrotechnical Commission (IEC) (World Standards Services Network, 1998). Both organizations are based in Geneva, Switzerland and operate according to similar rules (World Standards Services Network, 1998). The ISO is a worldwide federation that facilitates standards development in the intellectual, scientific, technical and economic fields. Electrical and electronic engineering standards fall within the scope of the IEC.

Regional standardization committees such as the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN) work in conjunction with the ISO and IEC. In many cases, the results of the standardization work of these organizations are integrated directly into the ISO/IEC system and appear in International Standards published by ISO or by IEC (World Standards Services Network, 1998). Key organizations include CEN, ETSI, and BSI (British Standards Institute).

CEN, European Committee for Standardization

CEN was founded in 1961 and develops standardization initiatives within Europe (World Standards Services Network, 1998). CENELEC, the European Committee for Electrotechnical Standardization, develops standards within the electrotechnical sector and functions within the CEN. The mission of CENELEC is to develop a coherent set of voluntary electrotechnical standards to serve as a basis to a Single European Market / European Economic Area, thereby, eliminating proprietary standards for goods and services within Europe (CENELEC, 1998).

ETSI, European Telecommunications Standards Institute

ETSI develops European standards in the telecommunications field and is at the forefront of issuing standards for multi-application smart cards. Several applications in the telecommunications area are using, or planning to use, the integrated circuit (IC) card. However, nearly all cards today are mono-application smart cards.

IC cards are currently used in payphones throughout Europe. Smart cards are targeted for use in the Terrestrial Trunked Radio network (TETRA) and for Digital European Cordless Telecommunications (DECT) and Universal Personal Telecommunications (UPT) (Bardenfleth, 1999). Multi-application smart cards are expected to be advantageous to the user and eliminate the need for individuals to carry one card for each application.

A comparison between ISO, CEN and ETSI shows that ETSI is in the forefront in standardizing the IC card (Bardenfleth, 1999). However, because of the close cooperation with the European Committee for Standardization (CEN), the application independent IC card standards for telecommunications use will be issued as European Standard EN 726 and called *Identification Card Systems - Telecommunications Integrated Circuits Cards and Terminals* (Bardenfleth, 1999).

ISO, International Organization for Standardization

Although there are several international standards concerning the development of smart cards, the main standards for smart cards are those developed by the International Organization for Standardization (ISO) (Chiew, Marston, Brodnax, Huvnh, Sigman, & Lumpkin, 1999). Table 1 lists the ISO standards that apply to contact cards. As described earlier, contact cards are smart cards that exchange data through a card reader.

	Table 1: Smart Card Normative Standards
ISO 7810	Physical Characteristics
ISO 7811	Recording Technique Magnetic Stripe and Embossing
ISO 7816	Integrated Circuit Cards with Contacts
ISO 10373	Test Methods
ISO 10536	Contactless Integrated Circuit Cards
ISO 11693	Optical Memory Cards – General Characteristics
ISO 11694	Optical Memory Cards – Linear Recording Method

Table 1. Smart Card Normative Standards.
Note. From *Smart Cards: A Guide to Building and Managing Smart Card Applications* (p. 31), by Henry Dreifus and J. Thomas Monk, 1998, New York, NY: John Wiley & Sons, Inc. Copyright 1998 by John Wiley & Sons, Inc.

The distinguishing characteristics of these standards are now examined.

ISO 7810

ISO 7810 establishes a baseline for the magnetic strip cards used worldwide for credit and debit applications. These standards also apply to the physical characteristics of smart cards. This standard defines the location for both the embossing and the magnetic strip. ISO 7810 also establishes the standard for the types of plastic and other material used to manufacture magnetic strip and smart cards (Dreifus & Monk, 1998). Table 2 outlines the specifications of ISO 7810.

Table 2: ISO 7810 Physical Characteristics of Cards

Materials: PVC, PVCA, or other materials having equal or better performance

Unembossed	*Embossed*
Outer Rectangle:	Outer Rectangle:
Card Width: 85.72 mm	Card Width: 85.90 mm
Card Height: 54.03 mm	Card Height: 54.18 mm
Inner Rectangle	*Inner Rectangle*
Card Width: 86.47 mm	Card Width: 85.47 mm
Card Height: 53.92 mm	Card Height: 53.92 mm

Thickness (all cards): 0, 76 mm +/- 0.08 mm

Table 2. Physical Characteristics of Cards.
Note. From *Smart Cards: A Guide to Building and Managing Smart Card Applications* (p. 32), by Henry Dreifus and J. Thomas Monk, 1998, New York, NY: John Wiley & Sons, Inc. Copyright 1998 by John Wiley & Sons, Inc.

ISO 7811

ISO 7811 is composed of four parts and establishes standards for the encoding of information on an identification card through embossing or magnetic strip techniques. According to Guthery and Jurgensen (1998), before online printing of transaction receipts became prevalent, merchants used imprinting devices to prepare credit card invoices and receipts. Therefore, the height and size of the embossed characters required standardization. ISO 7811-1 standardizes font sizes for recognition by optical devices.

ISO 7811-2 specifies the recording technique used to encode characters into the magnetic strip affixed to the card. Standards are in place for the three types of information stored on the magnetic strip. These are referred to as Tracks 1, 2 and 3. According to Guthery and Jurgensen (1998), both Track 1 and Track 2 are write-once/read many channels. Track 3 is a write-many and read many track. Each track

contains a longitudinal redundancy check character that is used by the card reader to detect errors in the information read versus what is originally written on the card.

ISO 7811-3 and ISO 7811-4 specify the location of the embossed characters and the location of the magnetic strips. Figure 2 illustrates the two areas for embossing. According to Guthery and Jurgensen (1998), the magnetic strip, if included, is found near the top on the back side of the card. The standard specifies that the magnetic strip and the embossing may not overlap.

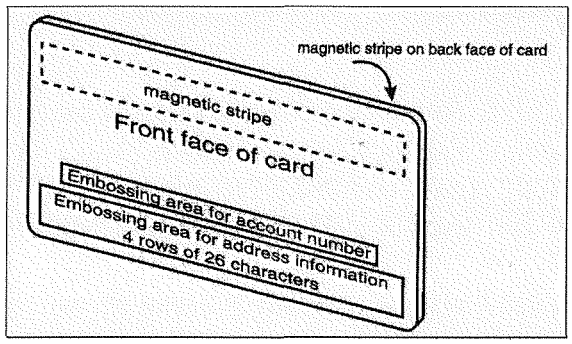


Figure 2. Embossing and Magnetic Strip Locations.
Note. From *Smart developers kit* (p. 39), by Scott B. Guthery and Timothy M. Jurgensen, 1998, Indianapolis, IN: Macmillan Technical Publishing. Copyright 1998 by Macmillan Technical Publishing.

ISO 7816

The basic contact smart card standard is the ISO 7816 series which is composed of six parts (Smart Card Industry Association, 1998). ISO 7816 is unquestionably the most widely known and followed general-purpose smart card standard (Guthery & Jurgensen, 1998). Standards for the ISO 7816 series are derived from the identification card standards and detail the physical, electrical, mechanical and application programming interface (Smart Card Industry Association, 1998). Table 3 lists the categories included in ISO 7816.

	Table 3: ISO 7816 Integrated Circuit Cards with Contacts
Part 1	Physical characteristics
Part 2	Dimension and location of the contacts
Part 3	Electronic signals and transmission protocols
Part 4	Inter-industry commands
Part 5	Numbering system and registration procedure for application identifiers
Part 6	Data elements for interchange

Table 3. ISO 7816 Integrated Circuit Cards with Contacts.

Note. From *Smart Cards: A Guide to Building and Managing Smart Card Applications* (p. 32), by Henry Dreifus and J. Thomas Monk, 1998, New York, NY: John Wiley & Sons, Inc. Copyright 1998 by John Wiley & Sons, Inc.

ISO 7816-1 describes the physical characteristics and defines the physical dimensions of contact smart cards and procedures that enable the smart card to resist impairment from radiation and mechanical stress. Additionally, the standard describes the physical location of an integrated circuit card's magnetic strip and embossing area (CardLogix, 1998). Part 1 also describes the environments in which the cards are expected to operate and the survivability within these environments (Dreifus & Monk, 1998). This part was changed to make it consistent with ISO 10373. ISO 10373 describes the testing of smart cards under extreme conditions such as heat or cold.

ISO 7816-2 defines the dimensions, electrical characteristics and location of the metallic contacts in addition to the meaning of each contact (CardLogix, 1998, Guthery & Jurgensen, 1998). According to Dreifus and Monk (1998), card manufacturers use unique patterns on the contact's surface to differentiate their products. Standardizing these

contacts ensures that cards work in card readers manufactured by various vendors. Figure 3 presents examples of contact designs from various vendors.

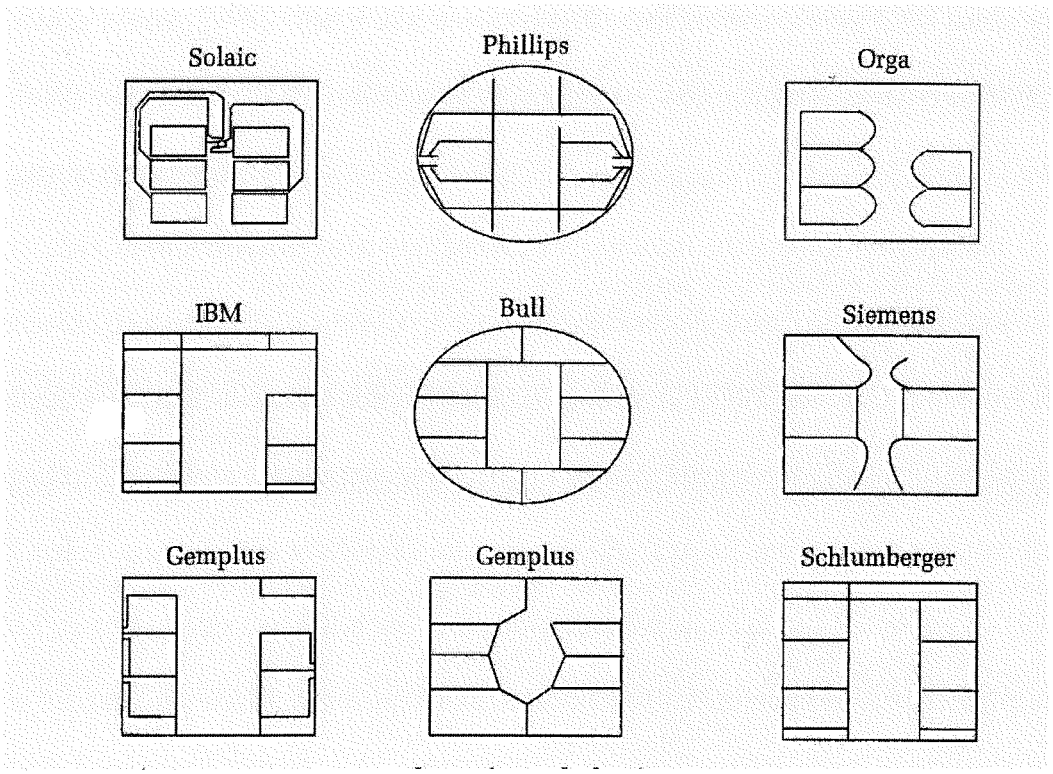


Figure 3. Examples of Module Design.
Note. From *Smart Cards: A Guide to Building and Managing Smart Card Applications* (p. 34), by Henry Dreifus and J. Thomas Monk, 1998, New York, NY: John Wiley & Sons, Inc. Copyright 1998 by John Wiley & Sons, Inc.

ISO 7816-3 discusses electronic signals and transmission protocols and the way a card and terminal communicate. In addition, Part 3 defines the voltage and current requirements for the electrical contacts defined in ISO 7816-2 (CardLogix, 1998). According to Dreifus and Monk (1998), early smart cards required 21 volts of programming power to establish a value in an EEPROM cell; today as few as 3 volts are needed.

ISO 7816-4 was first published in September, 1995 and describes the inter-industry commands for the exchange of information between a card and a card reader (Dreifus & Monk, 1998). Part 4 also establishes a set of commands for CPU cards across all industries and defines the commands to read, write, and update (CardLogix, 1998, Guthery & Jurgensen, 1998).

ISO 7816-5 discusses the international application numbering systems and registration procedure for a specific smart card application. Part 5 also establishes standards for Application Identifiers (AIDs) (CardLogix, 1998). An AID is composed of two parts. The first, a Registered Application Provider Identifier (RID), consists of five bytes and is unique to the vendor (CardLogix, 1998). The second part is a variable length field of up to 11 bytes that RIDs use to identify specific applications (CardLogix, 1998). When the card is inserted into a card reader, the identification number discloses the card's specific application. As multiple application cards proliferate, the card reader must be able to determine which application is requested. Therefore, in the near future, identification numbers will be crucial to smart card performance.

ISO 7816-6 describes the inter-industry data elements and defines the data encoding rules for applications (Guthery & Jurgensen, 1998). In addition, this standard details elements such as personal identification number (PIN), name and expiration date that can be manipulated by a smart card microcontroller (Dreifus & Monk, 1998).

As noted, ISO 7816 delineates smart card physical requirements. However, smart card application requirements are not defined. The lack of a single industry standard is a constraint on market growth (Chiew, Marston, Brodnax, Huvnh, Sigman, & Lumpkin, 1999). Although there is a global standard, several companies have formed alliances to

define smart card specifications and standardization, product interoperability, and an open platform. These companies include MasterCard, Motorola, Hitachi and Visa.

ISO 10373

ISO 10373 addresses reliability and quality assurance testing of smart cards. The standard defines exposure specification limits to electromagnetic phenomena such as x-rays, ultraviolet light, electromagnetic fields, and static electrical fields. Ambient temperature of the card is also described (Guthery & Jurgensen, 1998). Table 4 lists the exposure limits for physical phenomena.

Table 4: Exposure Limits for Physical Phenomena

Phenomenon	Limit
Ultraviolet light	Ambient (depends on card vendor)
X-rays	Two times acceptable annual human dosage
EMI - Electromagnetic Interface	No interference with magnetic strip
Electromagnetic fields	Less than 1,000 0e
Static electricity	1,500 volt discharge through 1.5 K ohm resistor from 100 pF capacitor
Heat dissipation	Less than 2.5 watt; card temperature less than 50° C

Table 4. Exposure Limits for Physical Phenomena.
Note. From *Smart developers kit* (p. 42), by Scott B. Guthery and Timothy M. Jurgensen, 1998, Indianapolis, IN: Macmillan Technical Publishing.

The standard also describes bending tests and torsion tests for assessing smart card flexibility. Torsion and bending tests address normal wear and tear on a card. For example, keeping the card in a wallet or purse may force the microchip connection wires to become damaged or broken. According to Guthery and Jurgensen (1998), experience

with these tests has shown that a 25 mm^2 microchip can routinely meet these flexibility constraints. Figure 4 illustrates the ISO 10373 card bending testing.

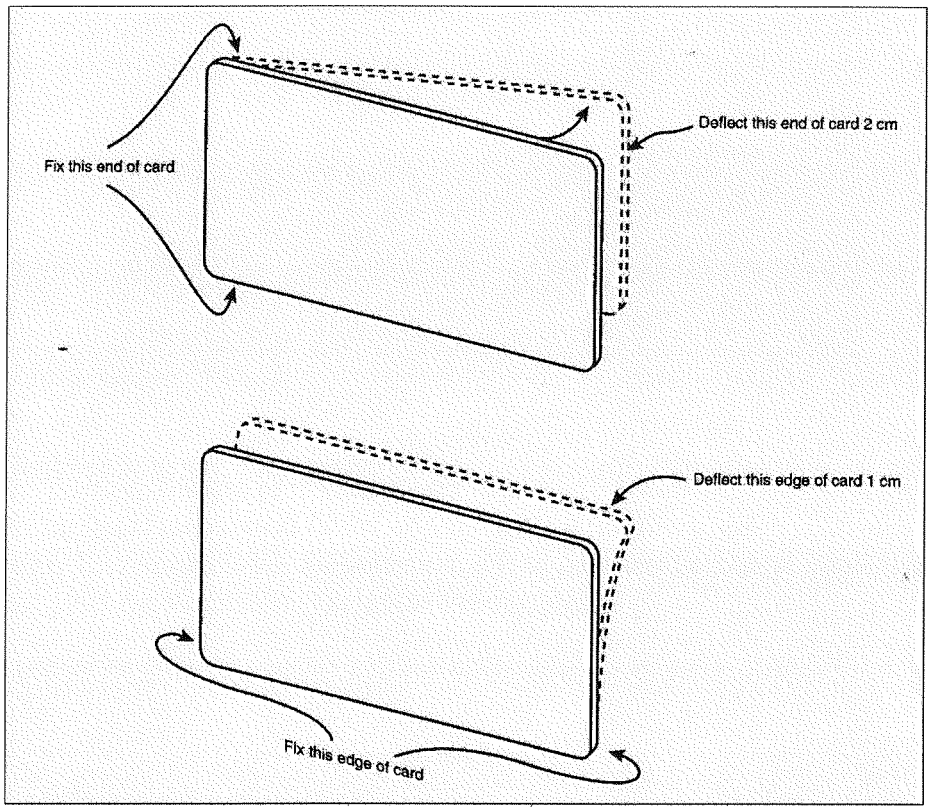


Figure 4. Card Bending and Testing.
Note. From *Smart developers kit* (p. 43), by Scott B. Guthery and Timothy M. Jurgensen, 1998, Indianapolis, IN: Macmillan Technical Publishing. Copyright 1998 by Macmillan Technical Publishing.

Figure 5 illustrates the torsion testing of a smart card.

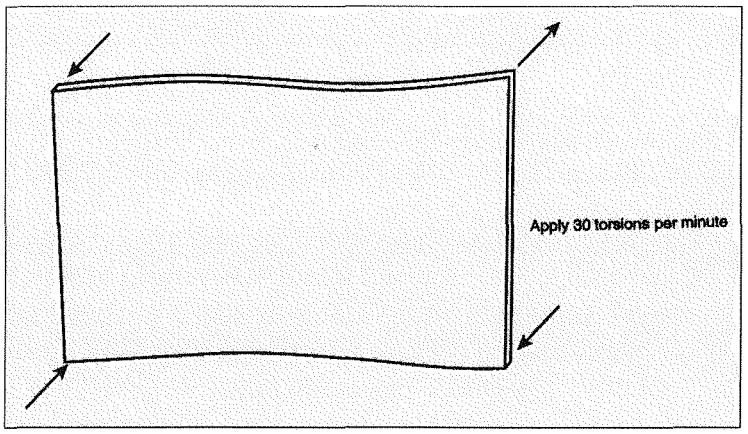


Figure 5. Torsion Testing of a Smart Card.
Note. From *Smart developers kit* (p. 44), by Scott B. Guthery and Timothy M. Jurgensen, 1998, Indianapolis, IN: Macmillan Technical Publishing. Copyright 1998 by Macmillan Technical Publishing.

ISO 10536

Contactless card standards are covered in ISO 10536. As described earlier, contactless smart cards transmit data through a built-in miniaturized radio modem and do not require contact with a smart card reader. Part 1 of ISO 10536 is identical to ISO 7816 and describes the physical characteristics of the smart card. Part 2 describes the location and size of the antenna or remote coupling areas. Table 5 lists the three types of contactless smart cards.

Table 5: Three Types of Contactless Cards

Immediate proximity
- Less than 1 mm distance from reader
- Less than 2° variance from vertical

Close proximity
- Between 1 and 2 mm distance from reader
- Specific orientation

Remote coupling
- Between 3 and 5 mm distance from reader
- No required orientation

Table 5. Three Types of Contactless Smart Cards.
Note. From *Smart Cards: A Guide to Building and Managing Smart Card Applications* (p. 38), by Henry Dreifus and J. Thomas Monk, 1998, New York, NY: John Wiley & Sons, Inc. Copyright 1998 by John Wiley & Sons, Inc.

Immediate and close proximity smart cards require that the reader/writer coupling device in the card and the terminal are precisely aligned. Additionally, these smart cards require a specific orientation of the card to the reader at very close distances (Dreifus & Monk, 1998). Remote coupling smart cards can operate within distances of a few centimeters to as many as 3 to 5 meters (Dreifus & Monk, 1998). The orientation of the card is not important and can be top up or top down as long as it is perpendicular to the read/write field.

ISO 11693 and ISO 11694

ISO 11693 and ISO 11694 define international standards for optical smart cards. According to Guthery and Jurgensen (1998), optical smart cards can be written once but read many times. These memory cards can hold between 1 MB and 40 MB of data.

ISO 11693 outlines the general characteristics of optical smart cards such as card construction, materials and exact dimensions. ISO 11694 defines the physical characteristics of optical smart cards such as height, width, thickness, and durability. The standard also addresses the optical card's dimensions and location of the accessible optical area.

De Facto Industry Standards

In response to the lack of technological standards within the smart card industry, consortia and alliances composed of corporations and multi-industry groups are developing technological smart card standards for consumers and merchants. Several de facto standards have evolved from these multi-industry liaisons. These de facto standards are now described.

EMV'96

In June 1996, EMV (Europay, MasterCard, Visa) published the EMV'96 Specifications Version 3.0 (Visa Specs EMV, 1999). EMV'96 is the ICC Specification for Payment Systems developed by Europay, MasterCard and Visa. The EMV acronym reflects the initials of the three bank card associations that developed the specification (Guthery & Jurgensen, 1998).

EMV'96 defines smart card transaction processing procedures and outlines the specifications for smart cards and terminals. EMV also defines how the application is expected to interact with the smart card (Guthery & Jurgensen, 1998). EMV'96 incorporates many of the standards defined by ISO 7816. These standards form the basis for global interoperability. EMV'96 specifications are maintained by Europay, MasterCard and Visa (Europay, 1998).

In addition, EMV describes procedures for electronic purse applications and interactions with universal multi-application smart cards. More importantly, EMV is the first detailed specification to describe smart card capabilities for handling multiple applications (Guthery & Jurgensen, 1998).

The primary goal of EMV is to promote established smart card industry standards for cards and terminals to foster global interoperability across competing payment systems (Europay, 1998). The EMV specifications include card, terminal, and applications requirements. These specifications are now described.

The EMV card specifications address electromechanical requirements; formats for commands; file and data structures; and processes relating to applications and security (Europay, 1998). Terminal and microchip specifications address the need for interoperability. As stated earlier, manufacturers have used unique patterns on the microchip contact's surface to differentiate their products. Standardization of these contacts ensures that cards function in card readers manufactured by various vendors (Europay, 1998). Applications specifications describe traditional payment transactions and electronic commerce transactions (Europay, 1998).

In June, 1999, Europay announced successful completion of the first cross-border transaction that demonstrates EMV-chip interoperability. An EMV-compliant MasterCard chipcard, issued by Barclays Bank in the United Kingdom, was successfully used in a transaction at a restaurant in Bratislava (Europay, 1999). This is the first time that a chipcard relying on the EMV standard was used for international payments outside the country of issue (Europay, 1999).

Java Card

The large number of incompatible development languages available for writing smart card applications deters design and utilization of smart cards. Proprietary protocols for operating systems were developed by individual card and semiconductor manufacturers for specific applications (Dreifus & Monk, 1989). As noted, ISO developed standards for smart cards and communication between smart cards and readers (ISO 7816). However, ISO did not develop standards for host to reader communications (Java Card Platform, 1999). Table 6 lists specific examples of operating systems for off-the-shelf smart cards and the cards' maximum memory size.

Table 6: Off-the-Shelf Operating Systems

Card Operating System	Manufacturer	Maximum Memory Size
Multiflex	Schlumberger	8 KB
MPCOS64K	Gemplus	8 KB
USCO48	US3	8 KB
OC100	Bull CP8	8 KB
I006.1	Orga	4 KB

Table 6. Off-the-Shelf Operating Systems.
Note. From *Smart Card Developers Kit* (p. 13), by Scott B. Guthery and Timothy M. Jurgensen, 1998, Indianapolis, IN: Macmillan Technical Publishing.

In 1997, Sun Microsystems introduced a Java smart card that enables developers to create Java smart card applications (Basch, 1998). The Java Card provides a standard set of application programming interfaces (APIs) and software classes than run on any existing smart card. Additionally, an application programming interface (API) is based on an easy-to-use and widely accepted programming environment (Dreifus & Monk,

1998). More importantly, the Java Card allows the application developer to hide the card-specific implementation of an application behind a standard set of methods. This capability allows the smart card application developer to create one set of software that can access many different types of cards and card readers (Java Card Platform, 1999).

A Java Card is a smart card that is able to execute byte code similar to the way Java-enabled browsers execute code (McGraw & Felten, 1999). Card Java is a subset of the standard Java language. With all of its libraries, standard Java is too large to fit on a smart card (McGraw & Felten, 1999). Card Java is a stripped down version of the standard Java language and is based on a subset of the Java API plus specific card commands.

As noted, Java gives developers a single cross-platform solution. The Java Card also provides a secure method for downloading updated applications and information to smart cards over networks (Kosiur, 1997). Java utilizes applets, or small pieces of code, designed to be downloaded onto a client machine from a remote host (Coleman, 1998). The applets are small enough to allow several to fit into the small amounts of memory available on smart cards. Because the applets are downloadable, the Java Card's functionality can be continually updated as new applications become available.

Additionally, McGraw and Felten (1999) state that Card Java provides developers with a more familiar development environment than the current unfamiliar smart card application languages. Java Card developers can build applications using standard, off-the-shelf, integrated Java development environments such as Symantec Cafe. These off-the-shelf development applications reduce coding time over traditional languages such as C++ by as much as 60% (Coleman, 1998).

According to Lemos (1997), Java Card promises to bring the benefits of a high-level language to the smart card industry. Additionally, Java Card simplifies programming applications and provides a large base of commercial development tools. Java smart cards allow multiple applications to run on a single card and enable users to independently download new applications onto a smart card (Taaffe & Johnston, 1997).

MULTOS (Multi-application Operation System)

A smart card operating system originally developed by Mondex International, MULTOS is an open, high-security, multi-application operating system (MAOS) for smart cards (MULTOS, 1997). MULTOS is designed as a universal operating system for smart cards and is viewed as complementary to Java (SJB Services, 1998). Just as developers write programs in the Java high level language for a Java interface, they also write programs in C high level language for a MULTOS interface (SJB Services, 1998).

The MULTOS interface runs on the MULTOS operating system and supports the Java interface (SJB Services, 1998). Additionally, MULTOS enables diverse products or services to reside securely and independently on a single card. As a benefit, cardholders use one card to perform multiple functions involving consumer loyalty programs, electronic cash services and telephone calling plans.

Maosco (Multi-Application Operating System Consortium) promotes MULTOS as the open industry standard. Maosco's members include Gemplus, Hitachi, MasterCard International, Mondex International, Motorola, and Siemens. Maosco also promotes an open, industry standard and a high security smart card multi-application operating system based on the MULTOS specification (MULTOS, 1997).

Smart Card for Windows

In October, 1998, the Microsoft Corporation announced its entrance into the smart card market with Smart Cards for Windows. Smart Cards for Windows enables card issuers and developers to use existing Windows expertise to develop and deploy a broader range of smart card applications than are currently possible with existing smart card systems (Microsoft, 1998).

According to Maki (1999), suppliers view Microsoft's proposed Smart Card for Windows operating system as the key to lending credibility to smart card technology, particularly, in the United States. For example, Schlumberger, the leading worldwide provider of smart card-based solutions announced that its Cryptoflex smart card is now interoperable with the Microsoft Windows 2000 operating system (Schlumberger, 1999).

Nelson (1998) predicts the use of smart cards for identification, security and Internet commerce will drive demand in the United States. Initially, Smart Card for Windows is focused on market categories such as secure log-on in the corporate sector, medical identification, electronic cash, and loyalty applications (Microsoft, 1999). Merrill Lynch is evaluating Smart Card for Windows. This company is also exploring smart card capabilities in providing traders and clients with secure access to account information (Simms, 1999).

Smart Card for Windows utilizes the specifications developed by the Personal Computer/Smart Card (PC/SC) Workgroup and combines smart card and computing platform technologies (PC/SC Workgroup, 1998). The software is a competitor to Sun's Java Card and MULTOS, the operating system developed for smart cards by the Maosco consortium (M'soft preps entry into smart cards, 1999). Microsoft's Smart Card for

Windows, Java Card and Multos support inclusion of several applications on the integrated circuit. Additionally, these operating systems allow changes to programs without affecting the other programs on the card (M'soft preps entry into smart cards, 1999).

According to Leung (1999), the widespread use of magnetic strip cards has slowed the growth of smart cards in the United States. Diana Knox, senior vice president of Visa USA, believes that the United States is five to ten years away from converting core debit and credit products to smart card technology (A rising tide of applications, 1998).

Smart Card Standardization Consortia

Although there is not a global smart card standard, companies and corporations are addressing smart card interoperability, standardization, open platforms and non-proprietary standard operating systems. These alliances are now examined.

Global Chipcard Alliance (GCA)

The Global Chipcard Alliance (GCA), a growing partnership of major corporations, promotes standardization and compatibility within the smart card industry (Watson, 1997). In October, 1996, PTT Telecom Netherlands, U. S. West, Bell Canada, GTE, and Telekom Malaysia founded the GCA. The mission of the GCA is to pursue industry standardization and compatibility (Global Chipcard Alliance, 1998). Today, the GCA includes more than 20 principal member organizations including IBM, Visa International, Siemens, Nortel and American Express.

Factors that contributed to the establishment of GCA included the proliferation of proprietary smart card programs and the need for standardization, compatibility and

interoperability (Global Chipcard Alliance, 1998). Smart card use is limited because the majority of smart cards and smart card devices are not usable outside the specific program for which they are developed. According to the Global Chipcard Alliance (1998), the most pressing issue that must be resolved is smart card interoperability between smart cards and components. Clearly, standards for smart cards, the chips that enable smart cards, host operating systems, card terminals, telephone networks, terminal equipment, and currency/currency conversion are indispensable in the smart card arena.

The Global Chipcard Alliance is developing an environment that accelerates the development of multifunctional smart card and chipcard technology and related applications. This is accomplished by establishing business alliances that support worldwide interoperability, public advocacy, endorsement of standards and specifications, and promotion of communications-enabled applications and solutions (Global Chipcard Alliance, 1998). Within the next three to five years, GCA predicts that smart card and chipcard consumers will access personalized applications and solutions regardless of time or location (Global Chipcard Alliance, 1998).

Smart Card Forum

The Smart Card Forum (SCF) is a non-profit, multi-industry organization working to accelerate the acceptance of multiple application smart card technology. The Forum was established in September 1993 and currently has 195 corporate members, including leading companies and organizations in banking, financial services, telecommunications, computer technology, health care, retail, and government (Smart Card Forum, 1999). Members include AT&T, Chicago Transit Authority, Cisco Systems, CyberMark, Inc., IBM and the General Services Administration.

True to its charter as a forum, the SCF supports member interaction and information exchange (Smart Card Forum, 1999). SCF's central focus is educating the marketplace and developing business propositions and positions on public policy issues. To accomplish its goals, the SCF has organized workgroups and committees. These groups explore and define smart card requirements in key sectors such as health care, retail, telephony, transportation, and travel and entertainment (Smart Card Forum, 1999). SCF members also promote interoperability, legal and public policy, multi-application smart cards, and network compatibility.

Recently, the Smart Card Forum expanded its membership to include the education sector (Smart Card Forum, 1999). The SCF states that college campuses are concentrated and closed communities that support multi-applications and can benefit from smart card deployment (Smart Card Forum, 1999). According to O'Sullivan (1999), college and university campuses provide the largest and most visible closed-system laboratory for smart card technology.

PC/SC Workgroup

The Integrated Circuit Card (ICC), or smart card, is an intrinsically secure computing platform ideally suited to provide enhanced security and privacy functionality for applications running within the personal computer environment (PC/SC Workgroup, 1996). Additionally, the ICC is capable of providing secure storage facilities for passwords, account numbers, private keys, and medical information. However, proprietary standards prohibit interoperability of ICC-based smart cards from various vendors. Currently, the use of these cards in the PC environment is hampered by a lack of

standards for interfacing PCs to Interface Devices (IFDs). Additionally, there is no standard operating system for ICC functionality.

The PC/SC (Personal Computer/Smart Card) Workgroup is a consortium of major industry leaders in the smart card-PC markets including Gemplus, Bull CP8, Toshiba, Hewlett-Packard, Microsoft Corporation, Schlumberger, Siemens-Nixdorf, Sun Microsystems, Verifone, and IBM. The PC/SC Workgroup addresses limitations in existing standards that complicate the integration of smart card devices with the personal computer. This group also develops solutions for integrating products from multiple vendors (PC/SC Workgroup, 1996).

The PC/SC Workgroup recently announced the release of version 1.0 of the PC/SC specifications. These specifications support the required interoperability necessary to promote the use of ICC technology in the PC environment (PC/SC Workgroup, 1998). Version 1.0 of the PC/SC specifications provides an overview of the minimum functionality required of ICCs, ICC IFDs, and PCs for enabling interoperability among elements provided by a variety of vendors (PC/SC Workgroup, 1998). These specifications ensure that smart cards, smart card readers, and computers manufactured by different vendors are compatible.

The PC/SC Workgroup (1996) has outlined six key objectives. These objectives are designed to:

- Maintain consistency with existing ICC-related and PC-related standards while expanding upon them where necessary and practical;

- Enable interoperability among components running on various platforms;
- Enable the use of advances in technology without rewriting application-level software;
- Enable applications to interface with products and components from multiple manufacturers;
- Facilitate the development of standards for application-level interfaces to ICC services to enhance the fielding of a broad range of ICC-based applications in the PC environment; and
- Support an environment that encourages the widest possible use of ICCs as an adjunct to the PC environment.

International Smart Card Initiatives

This section of the literature review presents international smart card initiatives. The use of smart cards in international commerce, telecommunications, travel and transportation, identification, and health care is described. Smart card utilization in the educational sector is also examined.

Introduction

A key reason for limited smart card growth in the United States can be attributed to the effectiveness of the telecommunications network infrastructure. In the 1970s and 1980s, the United States' credit card industry readily authorized and verified cardholder transactions quickly. A low-cost telephone connection interfaced to an electronic database containing the credit card holder's data for authentication of transactions (Allan & Kutler, 1997).

In terms of credit cards, Europe has a less sophisticated telecommunications infrastructure for credit card authentication, particularly in France where smart cards originated (Kaplan, 1998). Additionally, each country has its own telephony system which makes cross-border communications extremely difficult. According to Kaplan (1998), the speed and cost of using a telephone line to access a remote data base for credit card authorizations were expensive and time consuming. To compensate for this problem, European markets utilized smart cards. The smart card held the necessary data to authorize the transaction at point of sale, thereby, eliminating the need for utilizing the telecommunications infrastructure (Allan & Kutler, 1997).

Smart cards worldwide are extremely popular. According to a 1998 survey conducted by Faulkner and Gray, Inc. for *Card Technology Magazine*, Europe represents 66.9% of smart card business, followed by the Asia/Pacific region with 17.5%; the United States with 12.7%; and the remainder of the world with 5.1% (Maki, 1999). As Maki (1999) notes, the 1998 Faulkner and Gray study revealed that prepaid telephone cards represent 75% of the smart cards sold worldwide; health care cards account for 9%; financial services account for 9%; wireless phones account for 5%; and other miscellaneous segments account for the remaining 2%.

According to a comprehensive industry research report, *The Smart Card*, published by SJB Research, 800 million smart cards were produced in 1996, of which 625 million were telephone cards (SJB Research, 1999). It is important to note that smart cards are utilized for other applications. For example, in France, 21 million banking cards are now smart cards that support credit and debit transactions (SJB Research, 1999). Germany has issued 78 million health cards that store health care insurance data,

payment responsibility, and entitlement benefits (Dreifus & Monk, 1998). The United Kingdom is beginning the rollout of 90 million chip-based credit, debit, charge and automatic teller machine cards (SJB Research, 1999).

Smart Cards and Electronic Commerce

Smart cards are well-suited for financial transactions. Information is stored securely on the computer chip and protected by encryption and authentication technologies.

The data on magnetic strip cards is highly vulnerable. For instance, a sophisticated method called skimming enables counterfeiters to copy information from the magnetic strip to another debit or credit card (Overview of smart card technology, 1999).

According to Dreifus and Monk (1998), electronic commerce is defined as any monetary transaction that occurs electronically. In an electronic commerce environment, the smart card identifies the card holder, electronically secures the link between the consumer and the merchant, and authenticates the form of payment (Dreifus & Monk, 1998). Smart cards are currently used for small purchases, thereby, replacing coins and dollar bills. Stored value card systems, called e-cash or electronic purses, are implemented worldwide. The use of smart cards for electronic commerce is now discussed.

Smart Commerce Japan

Smart Commerce Japan (SCJ) is a consortium of 32 companies established to develop electronic commerce technology. Members include Japan Airlines, Asahi Bank, Memorex Telex Japan, Ltd., and Nippon Telephone and Telegraph Corporation. As part

of the Ministry of International Trade and Industry's (MITI) Electronic Promotion Program, SCJ is exploring the use of IC cards in the virtual mall environment (Smart Commerce Japan, 1998). According to Visa International (1999), nearly 30,000 Visa cardholders in Kobe have received advanced chip cards.

With Smart Commerce Japan, credit and stored-value are integrated and controlled by a single chip on a multi-application bank card (Visa, 1999). Smart Commerce Japan is the first program of its kind in Asia, and one of the first in the world to use stored-value smart cards for Internet purchases (Visa, 1999). Participating cardholders utilize a chip-based multi-application bank card that combines the Visa credit card and reloadable Visa Cash stored-value functions.

Consumers shop with Visa chip cards in both the physical world at a wide variety of merchant locations, and on the Internet through personal computers and special public kiosks offering Internet access. Cardholders choose between the Visa Cash card's credit function or the stored-value function. Cardholders can reload value onto their smart cards using special automatic teller machines (ATM) placed throughout the Kobe, Japan area (Smart Commerce Japan, 1998).

Smart Commerce Japan IC cards are accepted by approximately 1,000 hotels, restaurants, and department stores in Kobe, Japan (Smart Commerce Japan, 1998). Merchants utilize chip-reading terminals to process transactions. All transactions are processed through Visa systems (Smart Commerce Japan, 1998).

To purchase merchandise from the virtual mall, an individual requires a Visa Cash card, a PC, a Visa-developed application, and a smart card reading device that initiates a purchase over the Internet (Visa, 1999). Additionally, cardholders make online credit

card purchases at special Internet kiosks placed in high-traffic department stores and train stations in Kobe. Consumers pay for purchases by inserting a Visa chip card into a smart card reader attached to a personal computer or Kiosk. All purchases are protected by the Secure Electronic Transaction (SET) protocol which safeguards payment card purchases made over open networks.

In October 1997, Smart Commerce Japan completed the world's first chip and electronic commerce transaction. Visa and Toshiba, along with technology providers CyberCash and IBM participated in the first Internet purchase. A Visa chip card was used to purchase a bottle of sake from an Internet mall merchant site (Visa, 1999).

Visa currently has chip card programs underway in nearly 30 countries. It leads the industry with more than 21 million Visa chip cards issued, including nearly 8 million Visa Cash cards (Visa, 1999).

MasterCard International

According to the Gartner Group, worldwide purchasing over the Internet will reach $20 billion by the year 2000, a 233 percent increase over the estimated $6.1 billion for 1998 (MasterCard International, 1999). To compete in the Internet commerce marketplace, MasterCard International developed the Complete Chip Solution, a turnkey strategy for helping members migrate approximately 600 million MasterCard credit and debit cards to a chip platform (MasterCard International, 1999).

MasterCard, partnering with Mondex International, adopted the MULTOS card operating system for its chip cards. MasterCard's electronic cash product, called Mondex, is based on smart card technology and offers an alternative to paying cash for goods and services (MasterCard International, 1999). Currently, Mondex cash is tested in

Canada, Hong Kong, New Zealand and Australia. Mondex electronic cash smart cards store and dispense cash electronically. Cash transfers of funds occur with the use of one telephony system or Internet link.

In May, 1999, MasterCard International announced the MYCAL Card Company is on schedule converting its entire portfolio of more than five million magnetic strip cards to multi-application smart cards (MasterCard International, 1999). MYCAL is an issuer, acquirer, and merchant of MasterCard International and the fourth largest retailer in Japan (MasterCard International, 1999). MYCAL's retail businesses include supermarkets, department stores, clothing outlets, cinemas, and restaurants.

According to MasterCard International (1999), MYCAL is issuing smart cards directly to consumers beginning in the fourth quarter of 1999. By December, 1999, MYCAL plans to migrate 540,000 Silver and Gold MasterCards to smart cards and proceed at a rate of over 200,000 cards per month reaching a total of 5.4 million chip cards by 2002 (MasterCard International, 1999).

Testing of the MYCAL smart cards is progressing along with the conversion of card terminals. The full program will be implemented with more than 400 retail stores and include more than 12,000 smart card terminals (MasterCard International, 1999).

Smart Cards and Telecommunications

Global System for Mobile Communications (GSM)

The Global System for Mobile Communications (GSM) is a standardized international mobile phone system based on digital transmission and cellular infrastructure (Zoreda & Oton, 1994). In early 1982, the Conference des Administrations Europeenes des Postes et Telecommunications (CEPT), comprised of 26 European

telecommunications providers, recognized the need for a standardized cellular network (GSM Association, 1998). Although business was increasingly conducted on an international scale, the communications industry focused on local cellular solutions, none of which was compatible (GSM Association, 1998). There were different cellular networks in each country. Phones could not operate across national boundaries.

In 1984 the GSM project received the endorsement of the European Commission, and, in 1985, Germany, France, Italy and the United Kingdom endorsed the project (GSM Association, 1998). In 1987, 13 countries agreed to deploy GSM technology (GSM Association, 1998).

The first GSM network was launched in 1992 with standards developed by the European Telecommunications Standards Institute (ETSI) (Mitchell, 1999). This digital cellular technology utilizes chip-based Subscriber Identification Module (SIM) cards that are inserted into cellular handsets. GSM subscribers are identified by SIM cards. Each SIM card holds a user's identification number, name, phone number, network provider and authentication key algorithm (GSM Association, 1998). The SIM card identifies the user to the network operator and allows for remote authentication and authorization of digital service within a home region or in a remote service area (Dreifus & Monk, 1998). In addition to user credentials, the SIM card contains applications issued by the network operator, for example, market news, reservations, and weather (du Castel, 1999).

According to the Dublin-based GSM Association, there are currently 140 million subscribers in about 130 countries, up from 70 million in 1998 (Souped-up SIM cards, 1999). As GSM use continues to grow in popularity, SIM cards are becoming increasingly important products for smart card manufacturers (Mitchell, 1999).

As SIM cards are upgraded with more memory, power and security, the mobile phone is evolving from a device used to make telephone calls to a data communications device. A recent application innovation allows users to add value to chip cards through handsets (Mitchell, 1999). The card value can be used to purchase goods or services at participating merchant locations.

SIM vendors manufacture chip cards that support several applications through the mobile handset. These applications support access to bank accounts, electronic mail, news and weather reports, and provide connectivity to interactive games (Souped-up SIM cards, 1999).

In April 1999, Visa International personnel performed the first download of electronic cash onto an electronic purse card utilizing a GSM mobile phone (Visa, 1999). To load value onto a Visa Cash card, the user inserts the card into a slot on the mobile phone, inserts a PIN, and specifies the amount of cash required. The service utilizes a customized Motorola dual slot mobile phone, the StarTAC D, the SIMphonIC SIM card created by De LaRue, and an m-Commerce Server developed by Logica (Visa, 1999). This service is available to 1,000 Barclaycard cardholders, the UK's largest credit card issuer. According to the director of relationship card initiatives at Visa South Africa, a mobile phone can perform the functions of an ATM by providing electronic cash and other information to consumers quickly and easily (Visa, 1999).

Smart Cards and Travel and Transportation

Smart cards are widely implemented in the travel and transportation sectors. Key initiatives are profiled in this section.

London Association of Train Operating Companies

The London Association of Train Operating Companies has introduced a smart card that replaces a magnetic strip card (Phillips, 1998). This smart card supports access to public transportation throughout the city of London. Customers pass the card over a radio-frequency scanner at turnstiles to debit cash from the card. When fully implemented, the London system will be the world's largest smart card ticketing system.

Seoul Bus System

In 1995, the city of Seoul implemented contactless smart cards for use in the bus system. Bus card validators were installed in the city's 250 buses and smart cards were issued to customers on a volunteer basis (Contactless smart cards in Seoul, 1998).

The contactless method allows the card to remain inside a purse or wallet during the transaction. The validator, or smart card reader, serves as a device for collecting the fare and is equipped to handle different fares for different routes (Contactless smart cards in Seoul, 1998). Information taken from the smart card reader at the end of the day is tabulated by the bus management system (Contactless smart cards in Seoul, 1998). Fares are automatically deducted from the card and deposited into the bank account of the appropriate bus company.

Hong Kong's Contactless Transit Card System

In 1996, major transport companies in Hong Kong implemented a common fare collection system that utilize advanced smart cards. The system includes 3 million reloadable, contactless smart cards that are waved in front of card readers at 400 fare-collection sites located in 14 mass transit stations (Guthery & Jurgensen, 1998). This system allows access to all modes of public transportation including trains, buses and

ferries. Eventually, the system will include access to city parking lots, retail stores, and pay telephones (Guthery & Jurgensen, 1998).

Smart Cards for Identification

Drivers' Licenses - Argentina

The province of Mendoza, Argentina implemented one of the first smart driver's license programs in the world in 1995 (The Gemplus Smart driver's license in Argentina, 1999). Prior to the implementation of the smart driver's license, only 30% of all traffic tickets were paid. Moreover, there was no system to track repeat offenders. Improper utilization of fraudulent drivers licenses increased dramatically.

With the smart driver's license, authorities can identify and monitor repeat offenders and control driving habits. The smart license maintains two types of data: permanent information and dynamic information. The permanent data is the information found on a traditional driver's license, specifically, name, address and license number (The Gemplus Smart driver's license in Argentina, 1999). Additionally, the license contains medical information such as blood type, biometric data, and health information. The dynamic information or temporary information is the driver's up-to-date profile and driving record (The Gemplus Smart driver's license in Argentina, 1999). Police officers utilize hand-held readers to access the data stored on the card and can either read the information from the chip or update the information when necessary (The Gemplus Smart driver's license in Argentina, 1999).

Drivers' Licenses - China

The Commercial Bank of China is launching one of the largest bank smart card programs in China. According to Davis (1999), the bank will issue between 1.5 million

and 2 million cards within 18 months, each with a chip and a magnetic strip. The chip includes a driver's license feature, thereby, allowing police officers equipped with terminals to record traffic violations on the spot. Cardholders pay fines using Visa's Interlink debit system (Davis, 1999).

Smart Cards in Health Care

Health care programs that utilize smart cards have been in place in Europe and Canada for several years. The Canadian Armed Forces Card allows Canadian Armed Forces physicians to store prescriptions. The Green Shield Smart Card used in Windsor, Ontario stores emergency medical and pharmaceutical information on smart cards. The New Brunswick Health Card stores information relating to drug therapy. The Health Information Register in Vancouver utilizes smart cards to store patients' medical information, making it readily available to physicians (Zoreda & Orton, 1994). In Germany, 78 million smart cards store health care insurance data, demographic information, payment responsibility, and entitlement benefits (Dreifus & Monk, 1998). Approximately 500,000 French citizens carry health care smart cards as well (Brainerd & Tarbox, 1997). Specific examples of health care smart cards are now examined.

Cardlink

The Cardlink project, supported by the European Commission, tests patient-held smart card medical records. The project is currently being tested in five regions in four European countries. This project examines smart card capabilities in providing access to healthcare irrespective of site, country, language and health care system (Cardlink, 1997).

The Cardlink pilot program provides each citizen with a portable medical record. The portable medical record ensures patients receive emergency medical care irregardless

of location or country by making all patient information readily available on the smart card for health care providers (Cardlink, 1997).

Health Cards in France

France-based GIE Sesam-Vitale, a health-ministry-backed organization, issued 58 million cards to households throughout France. The cards contain demographic and insurance information (Balaban, 1999). Physicians use the card to access patient insurance records and electronically file claims.

Smart Cards as Interfaces for People with Disabilities

Self-service terminals such as Automatic Teller Machines (ATM) and ticket selling machines are becoming more prevalent in today's society. As these terminals become more complex and offer more services, the elderly and disabled find them more complicated to use. The SATURN project, supported by the Commission of the European Union through the Technology Initiative for Disabled and Elderly (TIDE), is studying the needs of disabled and elderly in relation to smart card systems (The SATURN Project, 2000). The project targets smart card usage in three areas: self-service terminals such as ATMs; public telephones; and public transportation.

Contact or Contacless smart cards will assist the elderly and disabled in completing financial transactions utilizing an ATM. A smart card with a stored user profile allows an individual to automatically select a preferred interface. The preferred interface may be a larger character display or reduced reflections from extraneous light to assist the elderly and visually disabled (The SATURN Project). Smart card usage to select a user interface is viable in public telephones and other self-service terminals such as ticket machines. Specific user interfaces may also include speech output, sound

amplification, visual display of sign language, braille output, and remote activation of an audible locating signal (The SATURN Project, 2000).

Public telephones present problems for individuals with hearing disabilities. Although public telephones have the facility for increasing audio amplification, smart card technology offers the capability of storing the user's preference for audio frequency (The SATURN Project, 2000). Additionally, individuals with poor manual dexterity find the keypad small and difficult to use. Smart card technology can automate dialing or force a touch window to open to make dialing easier.

Contactless smart card technology can also assist individuals in wheelchairs with public transportation. A wheelchair user may use a contactless smart card to alert the bus driver and to trigger the extension of the wheelchair ramp (The SATURN Project, 2000). Additionally, a similar smart card could trigger an audio message beside the door giving the destination of the bus for visually impaired passengers (The SATURN Project, 2000).

As many countries introduce legislation to protect the rights of handicapped individuals, service providers may need to re-evaluate the way ATMs and self-service terminals are utilized. Smart card technology may provide the interface required to make these terminals accessible to the disabled population.

Smart Cards in Higher Education

The first university smart card experiment occurred in 1983 at the University of Paris (Zoreda & Oton, 1994). The card stored the academic curriculum of the holder and offered a number of services within campus facilities (Zoreda & Oton, 1994).

In July, 1992, a smart card system was installed at the University of Calgary to control photocopier usage in the University library (Blackburn, 1993). After students at

the University successfully copied the contents from the photocopier card's magnetic strip onto the fraudulent photocopier cards, they fraudulently enjoyed unlimited free copying privileges.

Current smart card systems include additional functionality and are capable of future expansion. For example, current systems include joint partnerships with financial institutions. These cards may be used at off-campus establishments. To protect students from the loss or theft of the value stored on smart cards, a personal identification number (PIN) may be required for purchase over a specific dollar amount.

University of Nottingham, United Kingdom

The University of Nottingham issued smart ID cards to 17,000 students and staff (Nottingham moves to the head of the campus card class, 1998). The card is accepted at university-operated cafeterias and shops at Nottingham and campus bars and copy machines. The smart card is expected to provide access to campus facilities and function as a debit card at nearby shops (Nottingham moves to the head of the campus card class, 1998).

City University of Hong Kong

The City University of Hong Kong's (CityU) campus card system supports a smart card that utilizes two chips (CityU, 1997). Called CitySmart, the card has a stored value function and serves as an identity card. The cash-dispensing function, controlled by a contact chip on the card, was developed by the University and Hang Seng Bank (CityU, 1997). Currently, the card is used for making purchases at on-campus locations. The second computer chip, a contactless chip, supports access to campus-based facilities such as the library, sports center and, laboratories (CityU, 1997).

University of Edinburgh, Scotland

The University of Edinburgh is the first university in Scotland to introduce a multi-functional campus smart card (University of Edinburgh, 1999). The card provides convenience to faculty, students and staff by combining all campus cards into one multi-functional card and reducing the need to carry cash on campus.

The University partnered with the Bank of Scotland to implement the chipcard's electronic purse function. Cash is added to the card and stored in the form of electronic cash (University of Edinburgh, 1999). The card is used to make small purchases at on-campus facilities. Future functionality includes the ability to purchase goods and services at off-campus facilities.

Domestic Smart Card Initiatives

In 1989, less than five percent of Americans had heard the term smart card (Woods, 1989). A 1995 study conducted by Payment Systems, Inc. (PSI), an internationally known research firm in the financial services industry, indicated the level of consumer awareness grew to 27 percent (Keenan, Rea & Hubbard, 1997). Balaban (1999) predicts that as the Microsoft Corporation makes its Smart Card for Windows operating system commercially available, smart card usage can be expected to climb.

This section of the literature review examines domestic smart card initiatives. The use of smart cards for identification and in sectors that include commerce, travel and transportation, and health care is described. Additionally, smart card utilization on university and college campuses is examined.

Smart Cards and Electronic Commerce

According to Dreifus and Monk (1998), electronic commerce is any electronic monetary transaction that replaces the physical exchange of money or checks. Although still in its infancy, electronic commerce is gaining momentum as technology evolves.

Tobin (1998) views e-commerce as one of the largest business opportunities in the smart card sector. As a consequence, there is an urgent need for organizations to issue, manage, and coordinate smart cards and smart card transactions. Kessler and Sheppard (1997) observe that electronic commerce has gained enough critical market mass to be taken seriously as an alternative to traditional commerce techniques.

Clearly, Internet commerce is sparking interest in smart card deployment. According to Kaplan (1998), credit card transactions are expensive to process and do not offer a cost-effective method for making small online purchases. Retailers pay a 3 percent to 5 percent transaction fee for purchases. However, the utilization of smart cards for small purchases can increase profit margins by eliminating the aforementioned fee. Several examples of e-commerce initiatives are examined.

Visa Cash on the Internet

In May, 1997, Visa and Bank of America began a six-month pilot program testing the utilization of Visa Cash chipcards for making purchases over the Internet (Visa, 1999). Participants load funds onto a Visa Cash stored-value smart card by inserting the card into a portable smart card reader directly inserted into the PC's floppy disk drive (Gold, 1998). To load funds, the participant utilizes a secure Web browser to log into the PC Load system and enters a Bank of America HomeBanking ID and password (Gold, 1998).

The Visa Cash card is used in place of cash at locations displaying the *Visa Cash* symbol. According to Gold (1998), Visa Cash has not been very successful in the United States because consumers see no real benefit over real cash. If the card is lost or stolen, the cash is lost.

Visa Cash in Celebration, Florida

Residents in Celebration, Florida have been introduced to the Visa Cash card. The Visa Cash card from SunTrust bank is a smart card that stores cash electronically and is available as either a reloadable or disposable card (Visa, 1999). The Visa Cash card can be used at participating merchant locations. Residents load value on the reloadable card at the SunTrust bank or at designated locations throughout Celebration, Florida. The disposable cards are pre-loaded with value in denominations of $5, $10, $20, and $50 and are discarded when there is no more value left on the card (Visa, 1999).

Wells Fargo

In April 1998, a group of Wells Fargo employees participated in an electronic commerce smart card pilot program. The program allowed participating employees to log onto the Internet, transfer funds from their banking accounts onto a smart card and use the card to shop online (Wells Fargo, 1998). According to Wells Fargo (1998), the WellsWallet enabled employees to shop at participating merchant Web sites and purchase goods and services; receive refunds; transfer funds between their bank accounts and their Mondex card; check deposit account balances; and view their last ten Mondex card transactions.

Smart card transaction technology on the Internet holds the greatest appeal for merchants selling low-cost items, such as information, subscriptions, games or music

(Wells Fargo, 1998). According to Wells Fargo, the smart card pilot program provides insight into how best to capitalize on the growth of electronic commerce using smart cards (MasterCard International, 1999).

Smart Cards in Travel and Transportation

Smart Cards for Electronic Toll Collection (ETC)

According to Ognibene (1996) smart cards used for electronic toll collection (ETC) have the potential to reduce labor and support costs, eliminate theft and fraud, and standardize ETC. Picado (1998) adds that ETC systems are an improvement over conventional toll collection techniques because these systems have the potential to eliminate queues at toll plazas, save fuel, enhance audit control and reduce mobile emissions and toll collection costs. With ETC equipment, a person is no longer needed to manually collect tolls at toll booths.

ETC utilizes a telecommunications link that operates at radio or microwave frequencies (Picado, 1998). Each vehicle is equipped with a transponder that recognizes a signal transmitted by a roadside antenna. An identification code, carried in the transponder, is exchanged with an off-vehicle processing computer. The computer uses the code to identify the account from which to deduct the toll. According to Ognibene (1996) this transaction occurs in less than half a second.

Maine Turnpike Authority - TransPass

The Maine Turnpike Authority (MTA) implemented an ETC system on more than 100 miles of interstate known as the Maine Turnpike. According to Brazel (1996), the TransPass is an active read/write unit called a transponder and is mounted on the dashboard of a car or truck. The transponder calculates the toll amount, verifies sufficient

funds, adjusts the account balance, and notifies the driver of a low or insufficient balance. According to Brazel (1996), shifting these activities to the transponder greatly reduces cost. The MTA expects to save $5 million each year with the TransPass (Brazel, 1996).

Florida Department of Transportation - SunPass

By the year 2000, nearly all of Florida's toll roads and bridges will be equipped with the SunPass ETC system (Florida Department of Transportation, 1999). The SunPass transponder is mounted on the car's windshield. As the vehicle proceeds through the SunPass lane, account balances are updated as tolls are deducted from the customer's prepaid account. According to the Florida Department of Transportation (1999), a single SunPass-only lane processes up to 1,800 vehicles per hour, 300 percent more than a manual toll lane.

Smart Cards for Identification

New Jersey Department of Motor Vehicles

The New Jersey legislature approved moving the state's driver's license program to chipcards. All licenses issued after mid-1999 are scheduled to be 32-bit microcontroller-based smart cards with sufficient space remaining for storage of personal information and programs that private businesses may implement (One small step, 1998).

General Services Administration (GSA)

The GSA Office of Smart Card Initiatives plans to set the standards for government-wide administrative and financial smart card applications. The team will first create a common card for applications such as entering buildings and logging on to networks (Dorobek, 1998). According to Dorobek (1998), the GSA expects that every federal employee will carry one smart card used for identification, building access,

network access, property accountability, travel, small purchases and other administrative and financial functions by the year 2001.

Smart Cards in the Health Care Industry

According to Brainerd and Tarbox (1997), the United States health care industry has not effectively utilized information technology to reduce administrative costs and healthcare fraud, although there is pressure to do so. Solutions explored to support cost reduction efforts include smart card technology (Sharpe & Warthen, 1997).

According to Sharpe and Warthen (1997), characteristics of a smart card make it an ideal solution for the health care industry. Additionally, a patient-held portable record can increase treatment quality, efficiency, and cost-effectiveness and reduce administrative workloads (Ruscitti et al., 1997).

According to Engelbrecht (1997), a smart card, used as a communication tool, can enhance the availability and quality of patient information. As noted by Zoreda and Oton (1994), health care smart cards can be utilized for identification and health payments. By holding relevant patient data, these cards can also support provision of necessary emergency treatment.

A recent study by the Institute of Medicine (IOM) revealed that 30 percent of patient visits and over 90 percent of Emergency Room encounters take place without access to the patient's record (Sharpe & Warthen, 1997). Additionally, in today's medical environment patients are unable to access and review their own health care data and correct erroneous information (Brainerd & Tarbox, 1997).

Medical smart cards are divided into six broad categories based on the type of information stored. These categories include insurance cards, emergency medical cards,

hospital admission cards, follow-up cards, Universal Health Cards, and health passport cards (Health Card Technologies, Inc., 1997). The card holds all of the patient's administrative data and is updated each time the patient receives service from the health care provider (Bull SC&T, 1999).

The security and convenience of smart cards present many advantages. For example, smart cards protect the privacy of patient records, assure patient identity, provide vital information in emergencies, track medications, and produce an audit trail for fighting fraud (Medical smart cards, 1998).

Medical smart cards appear to be a successful method of storing patient records. Additionally, smart cards can potentially increase the security of patient records. Sharpe and Warthen (1997) explain that data stored on the smart card is not on-line and can only be viewed at the patient's discretion. Distinguishing characteristics of the health care smart card include its ability to transport confidential data from cardholder to practitioner and its convenience in making the data available immediately (Brainerd & Tarbox, 1997).

Miller (1993) identifies several security features that protect the information stored on the smart card. Because both the smart card and a secret code are required for system access, the security scheme is strengthened. Smart cards do not reveal their secret serial numbers or user passwords and are difficult to counterfeit. Smart cards can detect tampering attempts to the chip by detecting light, low or high voltage, slow clock speed, and/or the erasure of data in special witness or dummy cells that are randomly scattered throughout the chip (Miller, 1993). Finally, the smart card chip provides segmented storage for highly personal data which is protected by a personal identification number and can only be opened by the patient (Sharpe & Warthen, 1997).

Privacy advocates argue that storing an individual's personal and medical history on a smart card create a major privacy vulnerability. According to Davies (1996), the existence of an individual's life in many unrelated databases is one important condition that protects privacy. When this data is brought together in one centralized location, namely a smart card, the individual's privacy is no longer protected. As noted by Davies (1996), data protection laws are inadequate to deal with the use of health identification cards.

Additionally, Schneier and Shostack (1999) note that there is little analysis of the security risks associated with smart cards. These authors note that, although smart cards are protected with encryption and algorithm technology, there is still vulnerability. There are several parties involved in a smart card-based system. These parties include the cardholder, the data owner, the terminal, and the card issuer. According to Schneier and Shostack (1999), if the card owner is not the data owner, the system is open to the possibility of attack. Davies (1996) argues that the potential for the abuse of computerized information is compelling. Therefore, the reduction in the number of parties using the smart card means that the risk of cross-application attacks are practically eliminated (Schneier & Shostack, 1999). These authors conclude that single application smart cards are less risky. A single application smart card reduces the number of parties involved and creates a simpler operating environment with less complexity and less potential for attack.

Health Passport - A Project of the Western Governors' Association

The Health Passport Project is the largest health care initiative in the United States for smart cards. The project has been conducted over two years in the cities of Bismarck,

North Dakota; Cheyenne, Wyoming; and Reno, Nevada (Health Passport, 1998). Implemented in the summer of 1998, the project ended in the fall, 1999.

An estimated 22,000 pregnant women, mothers and children, eligible for care under public health programs, took part in the program (Health Passport, 1998). The program demonstrates how patients utilize smart cards to provide current information to health care providers. Additionally, the program determines the effectiveness of smart cards in improving access to health care.

The Western Governor's Association identifies several important goals for this program (Health Passport, 1998). These goals include reduction of health care costs by providing accurate information where it is needed, and when it is needed. In addition, this program is designed to improve the quality of care by giving patients better access to the care for which they are eligible; giving patients better control over information by reducing duplication of records; and ensuring customer satisfaction with health services.

Veterans Affairs (VA) Health Information Card

The VA's HomeCare program in Charleston, SC is piloting a program to store medical records on smart cards (Jackson, 1999). The purpose of the pilot program is to determine the usefulness of having a patient's medical information electronically available to the health care provider. Veterans requiring treatment after hours utilize area hospitals and clinics. The area hospitals and clinics must verify patient eligibility with the VA before patient records can be received. The smart card provides insurance information and supplies the patient's medical records immediately (Jackson, 1999).

Smart Cards in Higher Education

Smith, Cunningham and Cunningham (1997) identify key factors shaping the campus card market. According to these authors

- The success of existing magnetic card systems has stimulated the demand for more services to be added to the systems;
- College administrators are continuing to explore operational cost reductions and new sources of revenue; and
- New technology is prompting educators to explore new ways of delivering higher levels of service.

Implementation Considerations

Frank (1999) argues that magnetic strip technology delivers services comparable to smart card technology. For example, the ISUCard, issued by Iowa State University, utilizes only magnetic strip technology. The ISUCard provides several functions such as an identification card for students, faculty and staff; access card; bank card; and declining balance card (Iowa State University, 1999).

The ISUCard provides entry to university facilities such as the recreation/athletic facility and access to the campus library. Additionally, students can make the ISUCard an ATM card by opening a checking account with Firstar Bank (Iowa State University, 1999). This option allows students to access ATM machines and make purchases at the University book store and selected merchants on and off campus.

Students activate a cash strip account, or declining balance account, with the ISUCard by depositing up to $50.00 at cash-to-card machines located throughout the

campus (Iowa State University, 1999). The cash strip account functions as real cash at university facilities.

The MIT Card is issued by the Massachusetts Institute of Technology (MIT). This card also utilizes only magnetic strip technology. The MIT Card provides access to food services, parking, and the library (Massachusetts Institute of Technology, 1998). All dormitories on campus are equipped with card readers for card access as well. The card contains a second magnetic strip that accommodates requirements of the University's declining-balance program. Food purchases can be made at selected off-campus merchants as well as on-campus merchants. Additionally, the card is used in on-campus laundry machines and vending machines.

The University of Delaware's UD#1 campus card system is also magnetic strip-based. In June, 1998, administrators at the University of Delaware partnered with the Wilmington Savings Fund Society, a banking institution with $1.5 billion in assets, for supporting access to a wide variety of banking services to students with their campus ID cards (Klie, 1999).

Students use the campus UD#1 card to purchase items at participating locations on and off campus (Klie, 1999). The multi-function UD#1 card is accepted for purchasing food, video games, services, parking permits, and phone services, (Klie, 1999). The card can also be used at the university pharmacy, Registrar's office, bookstore, and recreational facilities. Additionally, the card stores meal plan information for both resident students and commuters.

As noted, smart card technology often incorporates magnetic strip technology. For instance, the University of Michigan's MCard utilizes magnetic strip technology as well

as smart card technology. However, the MCard provides similar services as the MIT Card, ISUCard and the UD#1 Card. The MCard serves as an access card, ATM card, debit card and library card (University of Michigan, 1999). The card's computer chip electronically stores up to $50.00 which may be spent at over 60 off-campus locations as well as used in copy and vending machines.

According to Frank (1998), there are no actual statistics, but industry experts estimate that approximately 1,200 to 1,300 of 3,500 colleges in the United States employ some type of campus card program. Many campuses support more than one card since each department may have issued its own card. For example, prior to the implementation of MIT's campus identification card, a separate card was required for library access. The MIT Card is now encoded with a unique library ID number to eliminate the need for a separate library card (Massachusetts Institute of Technology, 1998).

Hale (1999) states that colleges and universities have utilized card-based systems for many years and some still have separate cards for each system. For example, the student identification card at Towson University in Towson, Maryland grants access to library materials. A machine readable strip affixed to the University ID card serves as library identification (Towson University, 1998). However, students utilize a separate card to access the dining hall and meal plans.

Prior to the introduction of the Stanford Card in 1995, the Leland Stanford Junior University maintained a multiplicity of single-purpose cards issued by a variety of offices (Printup, 1997). For example, students required a library card, an access card for dormitories, and a third card for the university meal plan.

Industry experts such as Frank (1998) maintain that campuses will continue to use magnetic strip card technology for the foreseeable future. According to Rigney (1998), however, while most campuses in the United States employ magnetic strip technology, an increasing number of universities are moving to chip cards or are at least requesting proposals for such programs. The move to chip cards is attributed to the number of applications and functions placed on smart cards (Rigney, 1998).

According to Frank (1998) magnetic strip technology, like smart cards, is utilized for stored value purchases at vending machines, photocopiers, laundries, and even off-campus merchants (Frank, 1998). Adams State College in Colorado utilizes magnetic strip technology for its Campus Card. The Campus Card is used to make purchases at most locations on campus such as the dining hall, food court, vending machines, photocopy machines, and laundry machines (Adams State College, 1999). Several kiosks are set up around campus for students to replenish the cash value on the card.

The California Institute of Technology utilizes a magnetic strip campus card for building access and purchasing. Students require a Caltech Campus Card to access campus libraries, dormitories, and science laboratories (California Institute of Technology, 1998). Additionally, students deposit cash at several Value Transfer Stations located throughout the campus. The card is used to make purchases at the university bookstore, dining hall, and campus cafes, as well as used in campus laundry facilities and photocopy machines.

In the fall of 1994, the University of Toledo adopted a one-card program utilizing magnetic strip technology (University of Toledo, 1999). The Rocket Card provides access to campus services and facilities, library privileges, and meal plans. The front of

the identification card contains the student's photograph, name and status. Additionally, the face of the card contains a barcode to allow check out of library books and access to all computers on campus. The back of the card contains a large magnetic strip used for point-of-sale devices, activity readers, and door access readers. A thin magnetic strip on the back of the card manages a declining-balance account used for purchasing photocopies and computer printouts. Students can activate the phone card option when applying for the Rocket Card.

Washington University in St. Louis, Missouri cannot justify the cost of a smart card system. The University will not renew the contract with its smart card supplier upon expiration (Thomson, 1999). The University concluded that the costs of smart card implementation are not justified by the benefits.

The success of smart cards on the college and university campus is debatable. According to O'Sullivan (1999), experience confirms that if smart card use is not mandatory, students do not use them.

However, according to Smith, Cunningham and Cunningham (1997), the college campus market offers one of the best opportunities for early adoption of smart card technology in the United States. The University of Michigan (UM) smart card effort demonstrates enormous success in closed-end applications (O'Sullivan, 1999). UM issued 40,000 smart cards in 1995 (Smith et al., 1997). To date, over 96,000 MCards are utilized by students, faculty, staff and visitors and over 100,000 cards will be issued when the program is fully implemented (University of Michigan, 1999).

The MCard is the University of Michigan's single-card program and combines many features including identification, library privileges, building access, meal plans,

long distance calling, debit card, and stored value all on one card (University of Michigan, 1999). The CashChip option conveniently stores up to $50.00 of cash. Students may make small value purchases at locations both on and off campus including gas stations, grocery stores and the university bookstore. The University is currently planning to expand the use of the CashChip option to include locations throughout the country (University of Michigan, 1999). Additionally, the University is working with the City of Ann Arbor, the Ann Arbor Transportation Authority, and the Downtown Development Authority to utilize the MCard for payment of parking and bus fare throughout the city (University of Michigan, 1999).

Florida State University (FSU) continues to implement its multi-application campus card system. The infrastructure includes 700 smart card readers placed throughout the campus. Several hundred vending machines are designed to accept smart cards. Approximately 35,000 smart cards have been issued (Berinato, 1997). The FSUCard utilizes both smart card and magnetic strip technology. The FSUCard is used for building access, meal plan access, and can function as a bank card, telephone calling card and electronic purse.

The SmartWorld Chip is a multi-application IC chip located on the front of the FSUCard and has the capability to store prepaid value (FSUCard, 1999). The card is accepted in drink and snack machines, photocopiers, microfiche copiers, laundry machines and laser printers. Potential future services for the SmartWorld Chip include use in Millennium Pay Phones, on and off campus merchant locations, and secure access to student records (FSUCard, 1999).

According to Frank (1998), some universities find it difficult to justify the cost of a smart card system since magnetic strip technology may perform the required functions. However, Pennsylvania State (Penn State) University aims to generate revenue from its smart card system. Penn State University receives transaction fees when its campus cards are used for stored value purchases at retail locations and vending machines. Penn State charges card-accepting merchants transaction fees for the purchases initiated with its ID+ identification card at on and off campus locations (CardTechnology, 1999). Merchants pay a 1.5% transaction fee that is split between the school and Pioneer Systems, a subsidiary of the Penn State Credit Union that administers the smart card funds pool (CardTechnology, 1999). The fees recover system implementation costs. The University's initial system implementation costs totaled $537,940 (CardTechnology, 1999). Of the $327,000 Penn State expects to receive in card revenues this year, 22.9% will be generated from lost card fees; 16.8% from transaction fees; 15.3% from calling card revenue; 11.8% from sponsorship deals; and 33.1% from miscellaneous sources such as payments from housing and food services offices for supporting student meal plans with the card (CardTechnology, 1999).

Smith et al. (1997) predict that universities will rapidly convert to smart card systems. Advancements in technology enable universities to install state-of-the-art multi-application card systems. These card systems allow students to enter residence halls, access grades and transcripts on-line, and make both off-campus and on-campus purchases. The University of Michigan's multi-application MCard serves as a photo ID and library card, provides building access and can be used as a calling card, debit card and ATM card. Additionally, the card is utilized for the campus meal plan and enables

students to make small purchases using the CashChip function. Smith et al. (1997) believe that smart cards play an important role in securely identifying students and delivering access to institutional services.

Summary of What is Known and Unkown About Smart Cards

1974 marked the acceptance of Roland Moreno's first patent and his founding of the Innovatron. Therefore, 1974 is considered to be the starting point of the contemporary smart card era (Zoreda & Oton, 1994). To date, smart card growth has occurred mostly in Europe. Due to vandalism and theft in the early 1980's, France's Public Telephone and Telegraph system began supporting a coinless public telephone system utilizing smart cards to hold a pre-purchased value (Dreifus & Monk, 1998).

Technological advances and reductions in manufacturing costs contribute to worldwide market growth. According to Dreifus and Monk (1998), next generation smart cards will not only serve as substitutes for cash but will provide added benefits. As noted by these authors, smart cards provide fraud control for credit and debit cards, physical and logical access control for buildings or computer systems, and storage of emergency medical information. Additionally, Dreifus and Monk (1998) predict that smart cards will be used to unscramble cable or satellite signals and for ticketless travel on airplanes, subways, buses, and trains.

The first university smart card experiment occurred in 1983 at the University of Paris (Zoreda & Oton, 1994). The card stored the academic curriculum of the holder and offered a number of services within campus facilities (Zoreda & Oton, 1994). In 1989, college administrators in the United States began to recognize the potential for smart card technology on campus. For example, Murray State University in Murray, Kentucky

issued 8,000 smart cards with photographs for student identification (Smith, Cunningham & Cunningham, 1997). In 1990 Loyola College in Baltimore, Maryland implemented a smart card system to manage its debit card meal plan for 3,000 undergraduate students (Blackburn, 1993).

According to O'Sullivan (1999), university campuses are ideal for smart card deployment. Smith et al. (1997) state that smart card technology is at the beginning of its life cycle. Smart card technology provides the ability to migrate to additional existing applications and to develop entirely new applications over the years. In order to be effective, campus card systems must be compatible with emerging bank card technology since it is evident that bank cards will evolve to smart cards (Smith, Cunningham & Cunningham, 1997). O'Sullivan (1999) believes that the success of smart cards on the college campus is a prediction of the success of smart cards in the United States.

Contribution This Study Will Make to the Field

This dissertation investigation contributes documented evidence of smart card utilization on college and university campuses. More specifically, through a case study research approach, this dissertation investigation evidences how universities and colleges have implemented smart card systems. Additionally, this investigation describes the benefits, limitations, and capabilities of smart card initiatives in higher education. Most importantly, through a case study research approach, this researcher formulates a paradigm for the development and implementation of smart card systems in higher education. The findings and conclusions of this dissertation investigation can be generalized to other academic institutions investigating the viability of a smart card system.

Summary

This chapter presents a detailed discussion of smart card capabilities, smart card technical fundamentals and smart card usage, both internationally and domestically. As smart card technology continues to evolve, chip cards are gaining acceptance in sectors that include electronic commerce, retail, travel and transportation, higher education and telecommunications.

Although smart card technology has been in existence for more than three decades, it is only now gaining acceptance. Declining costs and acceptance of smart cards by different industries contribute to the recent market growth. This chapter describes specific examples of smart card usage in business, healthcare, government and education. This information presents the reader with the foundation to understand the future trend of smart card technology.

Chapter III

Methodology

Research Methods to be Employed

The research design for this dissertation inquiry is a systems analysis approach in conjunction with a case study approach. Whitten, Bentley and Barlow (1994) describe the systems development life cycle (SDLC) as the framework for information systems development. Additionally, the SDLC is a management tool used to plan, execute, and control systems development projects (Whitten et al., 1994).

The classic form of the SDLC consists of four phases. They are systems analysis, systems design, systems implementation, and systems support. Modern variations of the SDLC have added a fifth phase, systems planning (Whitten et al., 1994). In this dissertation, a modern systems development life cycle (MSDLC) is complemented with a case study strategy (Yin, 1994) to develop a paradigm for a university-wide smart card student identification system.

The first section of this chapter examines the MSDLC model. According to Whitten et al. (1994), the MSDLC approach to systems development follows the classic problem solving paradigm:

- Identify the problem, opportunity or directive;
- Understand the problem's environment and the problem's causes and effects;

- Define the requirements of a suitable solution;
- Identify alternative solutions;
- Select the best solution;
- Design and implement the solution; and
- Observe and evaluate the solution's impact. Refine the solution accordingly.

In terms of this dissertation investigation, the solution is identified as a campus-wide, smart card student identification system. The MSDLC provides a realistic and structured development approach to the design and development of the campus-wide smart card student identification system.

Modern Systems Development Life Cycle (MSDLC) Methodology

According to Whitten et al. (1994), a systems development methodology ensures that a consistent and reproducible approach is applied to all projects. For this dissertation inquiry, this researcher utilizes a Modern Systems Development Life Cycle (MSDLC) methodology. The MSDLC methodology consists of five phases (Figure 6). They are:

- Systems planning. The planning phase identifies and prioritizes the information systems that return the most benefit to the organization, as a whole (Whitten, et al., 1994).
- Systems analysis. The analysis phase analyzes the business problem and defines the business requirements for a new or improved information system (Whitten, et al., 1994).
- Systems design. The design phase uses a computer-based, technical solution for the business problem identified in systems analysis (Whitten, et al., 1994).

- Systems implementation. The implementation phase constructs, assembles and delivers the new information system into operation (Whitten, et al., 1994).
- Systems support. Systems support sustains and maintains the system for the remainder of its useful life (Whitten, et al., 1994).

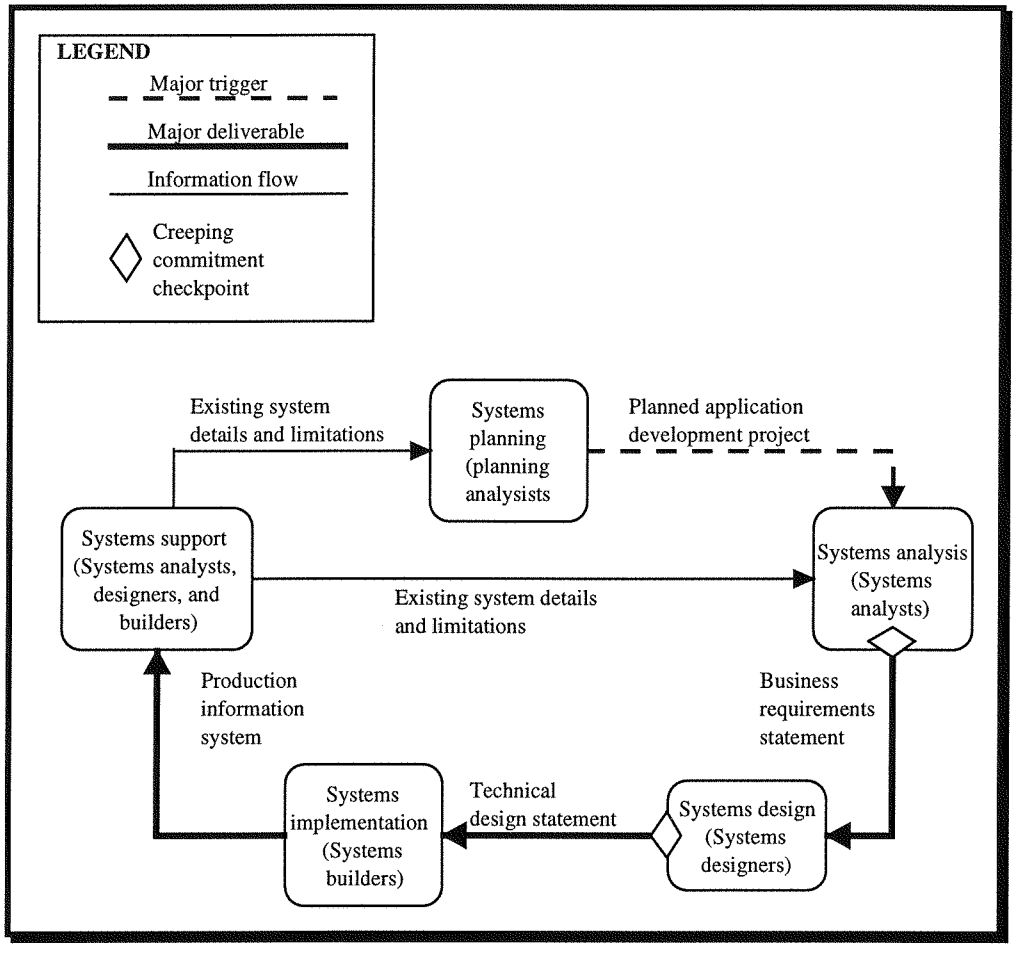


Figure 6. Modern Systems Development Life Cycle Methodology
Note. From *Systems Analysis & Design Methods, 3rd ed.* (p. 100), by Jeffrey L. Whitten, Lonnie D. Bentley, and Victor M. Barlow. 1994, Boston, MA: Richard D. Irwin, Inc.

Systems Planning

According to Whitten et al. (1994), systems planning identifies and prioritizes those technologies that return the most value to the organization as a whole. Systems

planning is also called strategic systems planning and information strategy planning. Strategic systems planning focuses on the use of information technology to add value to the organization, streamline business processes, and gain competitive advantage (Whitten et al., 1994).

Systems owners, comprised of executive management and higher-level middle management, drive the systems planning phase. The key facilitator of the planning phase is a planning analyst. According to Whitten et al. (1994), planning analysts possess a unique blend of skills and experiences in business management, systems analysis and design, data management, and networking.

In terms of this investigation, the systems planning team at Nova Southeastern University consisted of management members from Administration including Finance, Student Affairs, Business Services and the Office of the Registrar. Additionally, management from Academic Affairs and Technology participating on the team included representatives from Network and Software Services and the Office of Information Technology. Members from Library Services, Security and Police Services also took part in this investigation inquiry.

The planning effort for smart card deployment at NSU consisted of three phases: identifying the business mission; defining the information architecture; and analyzing the organization (Whitten, et al., 1994). The systems planning phase as described in Whitten, Bentley and Barlow's (1994) Modern Systems Development Life Cycle Methodology provided the framework for the planning phase.

Study Phase - Identify the Business Mission

According to Whitten et al. (1994), if information systems are to truly return value to the business, they must be aligned with the business mission. The systems planning phase for this dissertation investigation involved documentation of a smart card paradigm in terms of NSU's mission, goals, objectives and requirements.

Nova Southeastern University is the largest independent institution of higher education in the Southeast and it is among the 20 largest independent institutions nationally (Nova Southeastern University Fact Book, 1999). The university consists of five campuses in the Miami-Fort Lauderdale area in addition to several owned and leased off-campus clinical facilities. The library system is comprised of the East Campus Branch Library, Einstein Library, Health Professions Division Library, Law Library, North Miami Beach Branch Media Union, Oceanographic Library, and four school libraries on the main campus. According to the university, 1998 enrollment totaled approximately 17,000 students pursuing undergraduate, graduate, and professional degrees.

The University's mission, as quoted from the Nova Southeastern University Fact Book (1999) follows:

> Nova Southeastern University is a dynamic, not-for-profit independent institution dedicated to providing high-quality educational programs of distinction from preschool through the professional and doctoral levels, as well as service to the community. Nova Southeastern University prepares students for lifelong learning and leadership roles in business and the professions. It offers academic programs at times convenient to students, employing innovative delivery systems and rich learning resources on campus and at distant sites. The University fosters inquiry, research, and creative professional activity, by uniting faculty and students in acquiring and applying knowledge in clinical, community, and professional settings (page iv).

According to Whitten et al. (1994), building a working partnership between information systems management and top business management is the key objective of the study phase. Additionally, the study phase establishes the importance of strategic systems planning and analyzes enterprise strategies that impact information systems. To successfully complete the study phase, executive participation is critical. Executives bring a full understanding of the business and the business mission.

Definition Phase - Define an Information Architecture

The definition phase defines an information architecture. According to Whitten et al. (1994), an information architecture is a plan that utilizes information technology to support the business mission. An information architecture is also called an information strategy plan or information systems plan. The information architecture includes the following elements:

- Data architecture. A high-level data model that identifies the data to be collected and the reports to be generated.
- People architecture. Defines the individuals in the organization and their location. The people architecture also identifies the management structure and how the proposed system will be supported.
- Process architecture. Identifies the business processes and highlights those processes that require redesign.
- Network architecture. Outlines the geographic locations of the business and the networks required to connect them.
- Technology architecture. Identifies and evaluates the technology opportunities.

The final output of the definition phase is an approved information architecture. In terms of this dissertation investigation, the deliverable is an information architecture for a university-wide smart card student identification system.

This smart card student identification system represents a single, unified identification and transaction card system. This paradigm combines magnetic strip technology with microprocessor chip technology.

As noted in the examination of smart cards, the microprocessor, or smart card technology, is traditionally used to manage money. Value is stored directly on the card, not in an online account accessed by the card. The card value is updated at reading devices attached to vending, copier, and merchant terminals. As we saw, card readers do not communicate with a host to process each transaction.

Therefore, the proposed NSU smart card student identification system integrates the new card with current university applications such as meal plan, library and access to buildings. The card offers new services such as banking, vending services and long-distance telecommunications.

Business Area Analysis

According to Whitten et al. (1994), the business area analysis (BAA) phase documents management's ideal vision of a highly streamlined and integrated system. In the BAA phase, management evaluates current processes for efficiency and attempts to redesign processes to increase efficiency prior to applying information technology.

Systems Analysis

According to Whitten et al. (1994), systems users are the key participants in the systems analysis phase. Users study the current business and information system and

define requirements for an improved system. Systems analysis consists of the following three phases:

- Survey phase. Also called the preliminary investigation. The survey phase defines the scope of the project.
- Study phase. The study phase analyzes the problems and opportunities that prompted the development of the project.
- Definition phase. The definition phase defines the users' requirements.

Survey Phase

The survey phase provides a basic understanding of the business scope and mission. According to Whitten et al. (1994), the survey phase establishes an initial reading of the problems and opportunities that triggered the investigation.

The survey phase for this dissertation investigation documents the problems and opportunities in terms of NSU's mission, goals, objectives and requirements. Much of the information for this phase was gathered from discussions with officials of the NSU Business Services Department.

NSU utilizes a traditional photo ID card that is primarily used for borrowing books and materials from the libraries. A second card is issued to students participating in the university meal plan. Additionally, the university utilizes separate declining balance cards for use in library photocopiers.

NSU has recently initiated discussion for a single student identification card to perform multiple applications. These discussions have occurred because replacement of NSU's meal plan system is imminent. Additionally, NSU recently broke ground for its state-of-the-art, futuristic library, research, and information technology center. These

factors are the impetus for the investigation of a university-wide, multi-application student identification card.

NSU Dining Plan

All undergraduate and graduate students, staff and faculty are eligible to participate in the NSU dining plan. All participants in the plan are issued a declining balance card that is used at point-of-sale (POS) registers. The POS register deducts the purchase from an individual's account. Replacement of this system is imminent. The system is DOS-based and is not compliant for use in the year 2000.

NSU Library, Research and Information Technology Center

In March, 1999, NSU began construction of a new library, research and information technology center. The center will offer electronic classrooms and online access to global databases, periodical research, and digitized collections. Additionally, the NSU technology center will partner with the Broward County Public Library system. The challenge for NSU is to offer an access card that differentiates NSU students from Broward county residents utilizing the technology center. The library/technology center is targeted for completion in December, 2000.

Smart cards offer significant potential in terms of NSU's library requirements. The partnership between NSU and the Broward County Public Library system requires librarians to distinguish between NSU students and Broward County residents. A smart card-based system enables the library to control access to specific services, modulate access and charges according to user profiles, provide an e-purse for financial transactions, and regulate Internet access.

The European Commission has been active in the support of research for innovative library services and tools. The Libraries Programme, launched in 1990, encourages the private sector to work with libraries to significantly increase the quality of resources available to the library user (Information Society Technologies, 2000). The benefits of smart card technology for total library management are illustrated by the Libraries Programme's TOLIMAC project.

The goal of the TOLIMAC (Total Library Management System) project aimed to develop a management system providing controlled access to networked information services in a library environment (Information Society Technologies, 2000). The TOLIMAC system is based on smart card technology and incorporates functionalities such as user identification, access control, authentication, and electronic payment (Information Society Technologies, 2000). The project addresses three key issues:

- Access control in libraries;
- Control of information resources; and
- Access to multiple resources, from multiple locations.

The TOLIMAC project effectively demonstrates the benefits of smart card technology in the management of library resources. The TOLIMAC concept provides an opportunity to control and manage access to resources and provides a demonstration of a solution for total library management.

Study Phase

The study phase provides an in-depth understanding of the problems and opportunities that exist with the current system. The findings of the study phase are documented in a business problem statement (Whitten et al., 1994).

Based on conversations with the Business Services Department, this investigator developed the following statement of problems and opportunities:

> Statement of problems and opportunities: Nova Southeastern University would like to pursue a comprehensive approach to implementing a single identification and transaction card program. The university is currently serviced by separate applications that are not well integrated and do not offer maximum efficiency and convenience for students, faculty and staff. Additionally, the university's declining balance meal plan system is a DOS-based system and is non-compliant for use in the year 2000. An opportunity exists for card technology in the new Library and Technology Center. The challenge for NSU is to offer an access card that will differentiate NSU students from Broward county residents utilizing the technology center.
>
> Expected solution: Nova Southeastern University envisions a single, unified identification and transaction card system that will be significantly more convenient for members of the university community. The common identification/transaction card will establish a single, common recognizable identification card for members of the university community. The card will increase effectiveness of campus-based systems by promoting card-based access to services. Finally, the card will establish a reliable mechanism to determine that the cardholder is currently registered or employed by the University and is eligible to access and receive university services.

Table 7 summarizes the problems and opportunities in terms of urgency, visibility, priority and possible solutions.

Table 7: Problem Statements

Brief Statement of Problem, Opportunity, or Directive	Urgency/ Visibility	Priority/ Rank	Proposed Solution
1. The university's declining balance meal plan system is a DOS-based system that is non-compliant for use in the year 2000	ASAP/ High	1	Quick fix; then new development
2. NSU does not utilize a multi application student campus card, but utilizes separate cards for campus functions	6 months/ Medium	2	New Development
3. The challenge for NSU is to offer an access card that will differentiate NSU students from Broward county residents utilizing the new technology center	3 months/ High	1	New Development
4. NSU multi-card applications are not well integrated to maximize efficiency and convenience for students, faculty and staff	6 months/ Medium	2	New Development

Definition Phase

According to Whitten et al. (1994), the definition phase describes the requirements of the proposed system and finalizes the project scope. The systems analyst and systems users are the key participants in this phase. The business requirement statement is the major deliverable of systems analysis (Whitten et al., 1994).

Based on conversations with NSU Business Services Department officials, this investigator documented the scope of the single-application student identification system. Table 8 outlines the potential scope of the proposed student identification card.

Table 8: Potential Scope of the NSU Smart Card System

	NSU on-line	Bank on-line	Off-Line
COMPUTING			
Printer fees			X
Access control	X		
Network Charges		X	
HOUSING/FOOD SVC			
Meal Plan/Dining access	X		
Residence hall access	X		
Vending			X
Laundry service			X
FINANCIAL AID			
Electronic applications	X		
Electronic payments		X	
COMMERCIAL USAGE			
Long distance phone			X
Banking		X	
Debit card		X	
ATM services		X	
Point of Sale (POS)	X		
Off-campus merchants		X	
On-campus merchants		X	
LIBRARY			
Book checkout	X		
Fine billing		X	
Copy service		X	
POLICE SERVICES			
Parking	X		
Fine/fee payments		X	
REGISTRAR			
Address update	X		
Phone registration	X		
Lab access	X		

Case Study Strategy

This researcher utilized the SDLC in concert with a case study strategy to conclude this dissertation inquiry. Yin (1994) states that the case study research strategy is a comprehensive strategy that comprises the logic of design, data collection and data analysis. Yin (1994) identifies five components of a research design that are especially important for case studies: 1) a study's questions; 2) its propositions, if any; 3) its unit(s) of analysis; 4) the logic linking the data to the propositions; and 5) the criteria for interpreting the findings.

The use of case study protocols to document and organize data collection is the most desired prelude to systematic data collection (Yin, 1977). Additionally, Yin (1994) states that the protocol contributes to increasing the reliability of case study research and is intended to guide the investigator to carry out the case study. A description of case study protocol for this dissertation investigation follows.

Case Study Protocol

Overview of the Case Study Project

By means of a case study approach, this researcher developed a paradigm for the development and implementation of smartcard systems in higher education. This case study focused on NSU in Fort Lauderdale, Florida. This researcher identified and documented answers to the following questions:

- How can NSU effectively implement a smartcard system to optimize the use of multiple application card access?

- How will NSU benefit from the implementation of a multiple application smartcard system?

The findings of this case study can be generalized to other academic institutions investigating the viability of a multiple application smartcard system.

Procedures

Yin (1994) defines case studies as studies of events within their real-life contexts. Additionally, Yin (1994) states that data are collected from existing people and institutions and not within the controlled confines of a laboratory, the structured limitations of a survey, or the privacy of a library.

To complete the major task of data collection, this researcher relied on focused interviews with key individuals instrumental in the development and implementation of smart card systems at colleges and universities. The National Association of Campus Card Users (NACCU) is open to all colleges, universities, secondary institutions and companies involved in the campus card market. This organization identified 25 college and university campuses currently utilizing smart card technology. This researcher conducted telephone interviews with key individuals at 23 of the 25 colleges and universities. Additionally, archival records were examined. All data obtained from these interviews were organized and documented in a separate case study database.

Case Study Questions

Yin (1994) states that, unlike questions in a survey, the case study questions are reminders of what information must be collected and are designed to keep the investigator on track as data collection proceeds. Based on the literature research and the goals and objectives of this dissertation investigation, a questionnaire consisting of 16 key

questions was developed (Appendix A). The questions were developed through joint efforts of this researcher and the Assistant Director of Business Services at Nova Southeastern University. To ensure clarity and validity, the questionnaire was reviewed by the Director of Business Services at Nova Southeastern University and members of the Research and Planning Department at Motorola Communications.

The questionnaire was administered to 23 of the 25 colleges and universities currently utilizing smart card technology on campus. Additionally, the questionnaire was administered via telephone to the key individuals responsible for the smart card system implementation.

Analyzing Case Study Evidence

Yin (1994) states that analysis of case study evidence is one of the least developed and most difficult aspects of researching case studies. Yin (1994) identifies two strategies for conducting case study analysis:

- Relying on theoretical propositions; and
- Developing a descriptive framework.

The questions asked in this dissertation inquiry provided the descriptive framework for organizing the case study analysis. This dissertation investigation involved multiple case studies. In addition to an analysis of each individual case, the process provided a cross-case analysis. In a multiple-case study, one goal is to build a general explanation that fits each of the individual cases, even though the cases vary in detail (Yin, 1994). The goal of this multiple-case study was to develop a paradigm for the implementation of a smartcard system on a college or university campus.

According to Yin (1994), one of the most desirable strategies for case study analysis is to use a pattern-matching logic. The pattern-matching logic compares an empirically based pattern with a predicted one (Yin, 1994). If the patterns coincide, the results strengthen the internal validity (Yin, 1994).

This dissertation investigation utilized an analytic strategy similar to pattern-matching called explanation-building. The goal of explanation-building is to analyze the case study data by building an explanation about the case (Yin, 1994). According to Yin (1994) the explanation, or proposal, contributes to theory-building.

In this dissertation investigation, the approach was applied to multiple case studies. This dissertation investigation utilized 23 case studies. Therefore, the result of the explanation-building process is also the creation of a cross-case analysis, not an analysis of each individual case.

According to Yin (1994), the explanation-building process is an iterative process and includes the following series of iterations:

- Making an initial theoretical statement or an initial proposition;
- Comparing the findings of an initial case against such a statement or proposition;
- Revising the statement or proposition;
- Comparing other details of the case against the revision;
- Again revising the statement or proposition;
- Comparing the revision to the facts of a second, third, or more cases; and
- Repeating the process as many times as is needed.

In this multiple-case study, the goal was to build a general explanation that fit each of the individual cases, even though the cases varied in details. In this dissertation

investigation, the general explanation is a documented paradigm for the development and implementation of a smart card system in a university environment.

Summary

The information presented in this chapter outlines the research methodology for documenting a paradigm for the development and implementation of a smart card system in a university environment. The case study approach ensured a gradual building of an explanation based on an actual set of multiple case studies. Based on this approach, a paradigm for smart cards in the university was developed that can be generalized to other academic institutions investigating the viability of a smart card system.

Chapter IV

Results

This chapter presents the findings obtained from targeted, focused telephone interviews with representatives from colleges and universities currently utilizing smart card technology. These findings contributed to the development of a documented paradigm for the development and implementation of a smart card system in a university environment.

Survey Analysis

This analysis section presents information obtained from case study interviews based on techniques described by Yin (1994). As noted earlier, a questionnaire consisting of 16 questions was administered via telephone (Appendix A). The data reflects responses from 23 college and university representatives.

As stated in Chapter I, the questions were developed through joint efforts of this researcher and the Assistant Director of Business Services at Nova Southeastern University. To ensure clarity and validity, the questionnaire was reviewed by the Director of Business Services at Nova Southeastern University and members of the Research and Planning Department at Motorola Communications.

Each survey question tested for specific variables. Statistical graphs documented the cross-case analysis and exposed similarities and differences between case studies. The documented analysis formed the basis for development of the paradigm.

Case Study Procedures

According to the NACCU, 25 colleges and universities utilize smart card technology (NACCU, 1999). It is these universities that this researcher targeted to participate in the case study survey.

A total of 23 of the 25 institutions were interviewed. This researcher initiated a telephone call to each of the institution's point of contact and requested participation in the case study survey. Two institutions declined to participate; 23 agreed. The following material presents case study survey material from the 23 participants.

Case Study - Size of the Campus Card Systems

The size of the colleges and universities that participated in the survey ranged from small community colleges to large state universities. Additionally, the number of smart cards issued and in circulation by each college or university ranged from 2,000 to 95,000 (Figure 7 and Table 9).

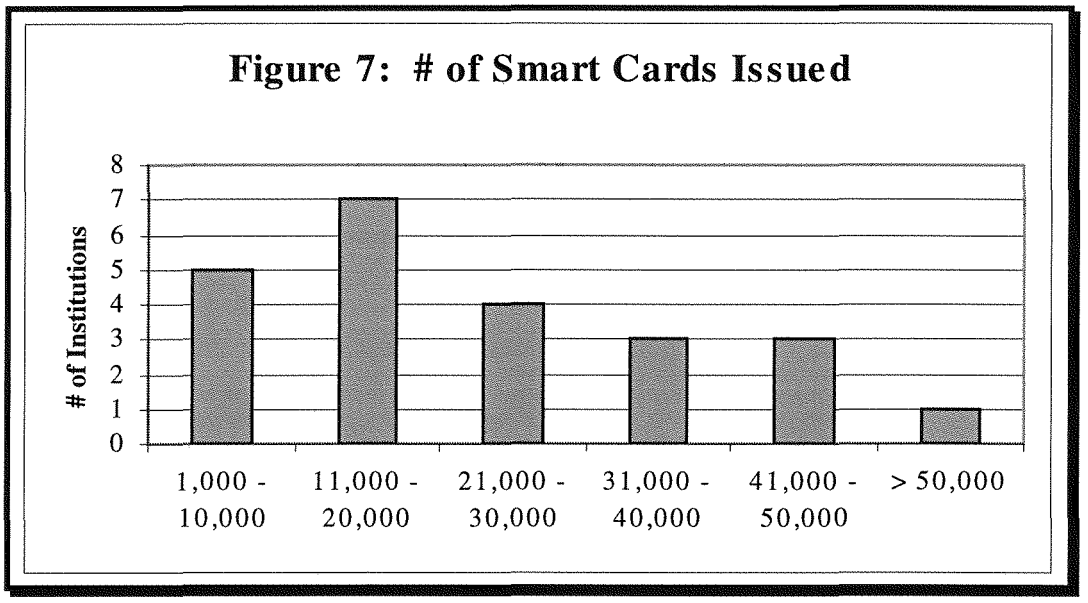


Table 9: Total # of Campus Smart Cards in Circulation

U1	2,000
U2	25,000
U3	15,000
U4	50,000
U5	49,000
U6	5,000
U7	31,000
U8	12,000
U9	21,000
U10	95,000
U11	7,000
U12	50,000
U13	3,000
U14	14,000
U15	15,000
U16	35,000
U17	18,000
U18	40,000
U19	28,000
U20	18,000
U21	13,000
U22	28,000
U23	3,000

Case Study Survey - Smart Chip Versus Magnetic Strip Technology

Question 1 tested for two variables: use of smart chip technology and the utilization of magnetic strip technology. As noted previously in the literature review, campus cards often incorporate smart card technology along with magnetic strip

technology. According to results from the cross-case analysis, 21 (95%) of the colleges and universities incorporated magnetic strip technology along with smart card technology; one university (5%) utilized only smart card technology.

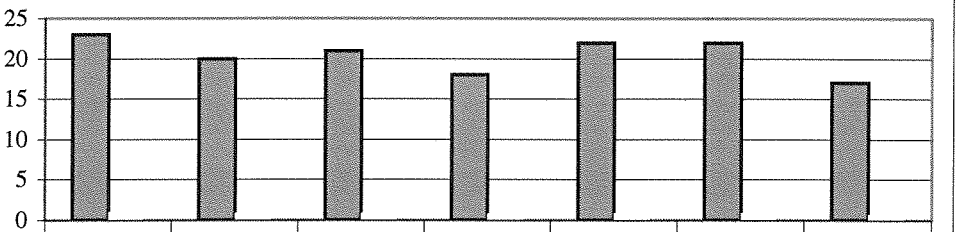
The major objective of a multi-application campus card is providing a multiplicity of services and functions on one card. This is accomplished by utilizing different technologies on the same card. The one-card approach is viewed as making a student's life easier and services more convenient.

Case Study – Campus Card Functions

A multi-application campus card provides a single, recognizable University identification card to students, staff and faculty. Question 2 of the case study analysis tested for various uses of the multi-application campus card. The case study surveys revealed the uses of multi-application campus cards included (Figure 8):

- Official university identification card;
- Access control card;
- Library card;
- Bank ATM card linked to an account at one of several participating financial institutions;
- Point of sale (POS) debit card;
- Stored value card or electronic purse; and
- Telephone calling card.

Figure 8: Uses for the Campus Card



	Student ID	Access	Library Card	Bank Card	POS Card	E-Purse	Phone Card
Yes	23	20	21	18	22	22	17
% Yes	100%	87%	91%	78%	96%	96%	74%

Interestingly, in all cases, the smart chip supported electronic purse applications only. However, the cards provided a multiplicity of functions and services. Each institution utilized technology that is appropriate to the specific service (Figure 9).

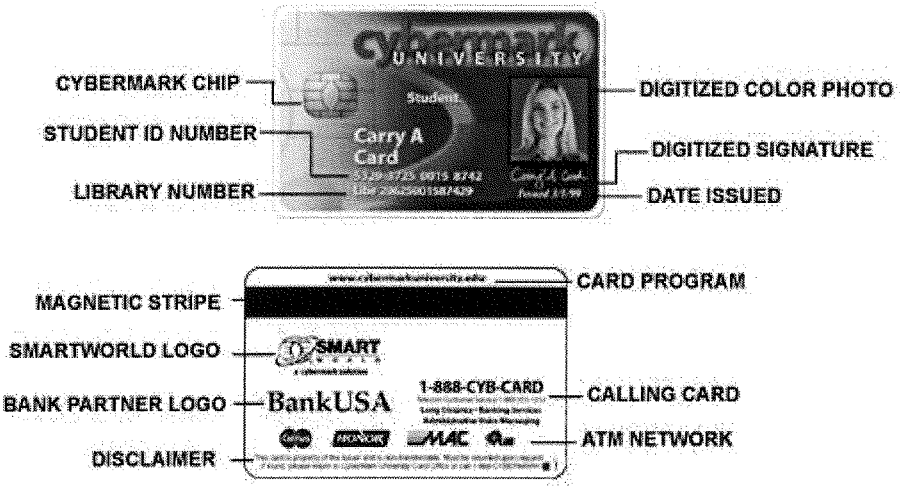


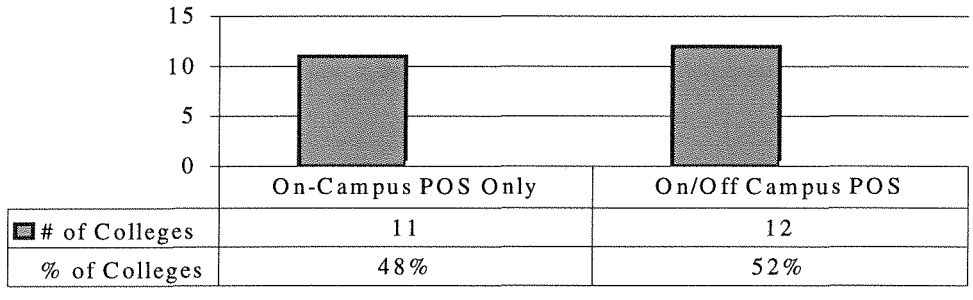
Figure 9. Cybermark Campus Card.
Note. From *About the Campus Card, http://www.cybermark.com*
Copyright 1999 by Cybermark.
Reprinted with permission.

Case study – Use of the Smart Chip

As previously stated, the smart chip is only used for electronic token applications. At 11 college campuses (48%), the smart chip is accepted by on-campus merchants and

vending areas only. All of these colleges indicated plans to expand card functionality to off-campus retailers. A total of 12 campuses (52%) partnered with off-campus merchants; the smart chip is accepted by on-campus vendors as well as selected off-campus vendors (Figure 10).

Figure 10: E-Purse - On-Campus vs On/Off Campus Purchasing



	On-Campus POS Only	On/Off Campus POS
# of Colleges	11	12
% of Colleges	48%	52%

Case Study - Managed Card Systems

Question 3 tested for the concept of managed card systems. A total of 22 (96%) universities interviewed selected one vendor to manage the campus card system. One university self-managed its campus card system.

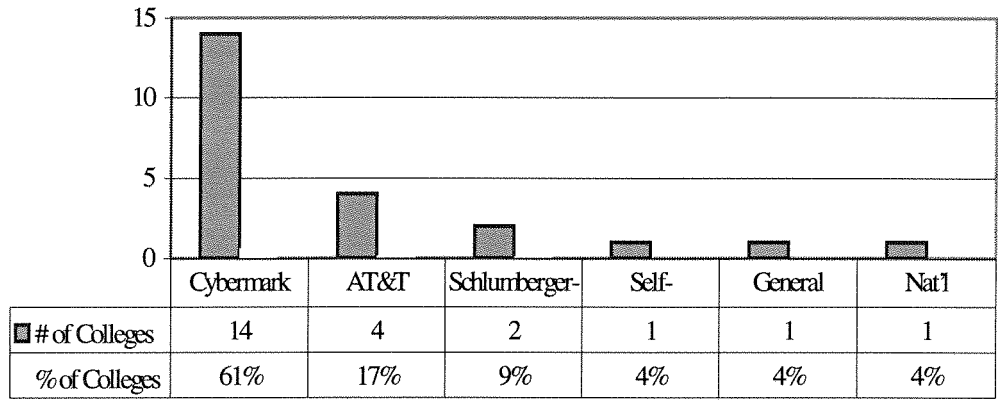
In a managed card system, the vendor is instrumental in the design, development, implementation and management phases of the campus card system. The functions of the vendor include:

- Assisting in planning and design;
- Integrating the multi-application card system with existing campus systems;
- Orchestrating mass card issuance;
- Identifying partner companies to complement the card program; and

- Providing applications with unlimited growth potential.

Cybermark is the industry leader in managed card systems installations and currently has fifteen university sites in North America. Cybermark tailors the multi-application card program to suit the university. Cybermark also provides assistance in hardware and software development and managed systems service. A total of 14 (61%) colleges interviewed chose Cybermark to manage their multi-application campus card system (Figure 11).

Figure 11: Managed Card System Vendors



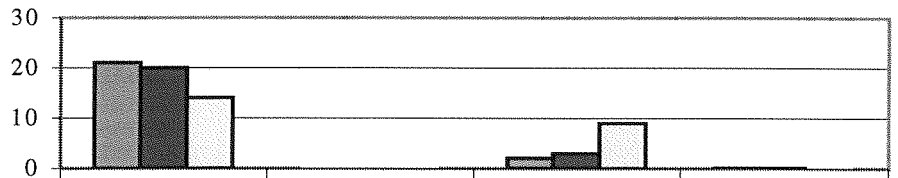
	Cybermark	AT&T	Schlumberger-	Self-	General	Nat'l
# of Colleges	14	4	2	1	1	1
% of Colleges	61%	17%	9%	4%	4%	4%

Case Study - Recognized Benefits

Question 7 tested for the recognized benefits of multi-application/smart card technology. The recognized benefits were:

- Revenue source;
- Safety of persons, and property; and
- Cost savings (Figure 12).

Figure 12: Recognized Benefits of Multi-Application/Smart Card Technology



	Yes	% Yes	No	% No
Revenue	21	91%	2	9%
Safety	20	87%	3	13%
Savings	14	61%	9	39%

When asked about the benefits of utilizing smart card technology, 21 (91%) stated that the multi-application card system was a source of revenue; 20 (87%) stated that the system had enhanced safety to persons and property; and, 14 (61%) stated that the system resulted in cost savings to the university.

Case Study - Recognized Benefits and Managed Card Systems

As part of the cross-case analysis, this researcher tested the significance of managed card systems with the recognized benefits. More specifically, this researcher tested and evaluated the Cybermark system with the recognized benefits. The stated hypothesis follows:

- A Cybermark-managed card system will likely contribute to:

    1. A revenue source;
    2. Safety of persons and property; and
    3. Cost savings.

    This researcher formulated three null hypotheses:

- A Cybermark-managed card system is not more likely to contribute to a revenue stream than other vendors' systems;
- A Cybermark-managed card system is not more likely to contribute to safety of persons and property than other vendors' systems;
- A Cybermark-managed card system is not more likely to contribute to cost savings than other vendors' systems.

To test the null hypotheses, this researcher utilized the chi-square test. Test results for two variables, revenue and safety, proved to be inconclusive; two of the four cells had less than 5 cases. According to Norusis (1991), the chi-square test should not be used if more than 20% of the cells have expected frequencies less than 5 or if any of the expected frequencies are less than 1 (Appendixes B and C).

The chi-square analysis was used to test the independence of two variables, savings and the managed card system vendor, Cybermark. More specifically, this test determined if managed card systems offer additional savings to the academic institution. In this case, the researcher tested the smart card solution provided by Cybermark.

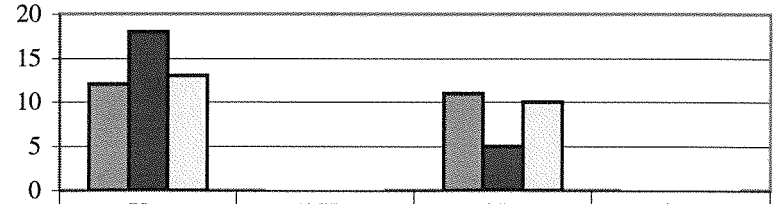
The observed significance level of the chi-square statistic was less than .05 (.03) (Appendix D). As a result, this researcher rejected the null hypothesis. The two variables, cost savings and Cybermark appeared to be dependent variables. Universities utilizing Cybermark as the managed card system vendor appeared to recognize additional savings associated with the multi-application campus card system. Additional testing of these two variables is warranted with a larger sample size.

Case Study - Partnering

Partnering with banks, merchants, and long distance carriers provides benefits to universities. Academic institutions receive revenue from participating merchants and financial institutions through ATM, point-of-sale, and smart card transaction fees. Additionally, long distance carriers pay a commission based on the overall calling card revenues from multi-application campus cards. These funds are normally used to cover system implementation and ongoing operating costs of the multi-application smart card system.

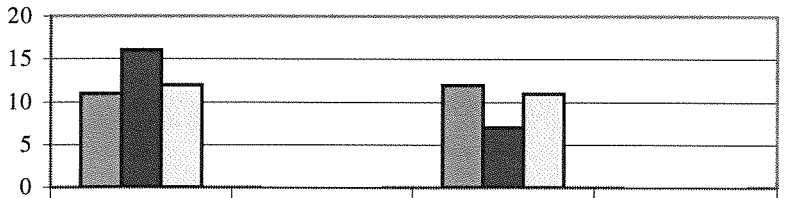
The case study survey revealed that 12 (52%) of the academic institutions partnered with off-campus merchants; 18 (78%) partnered with financial institutions; and, 13 (57%) partnered with long distance telecommunication carriers (Figure 13). Additionally, 11 (48%) of the colleges and universities realized revenue from partnership with merchants; 16 (70%) realized revenue from bank partnerships; and 12 (52%) realized revenue from partnerships with long distance carriers (Figure 14).

Figure 13: Partner Sources



	Yes	% Yes	No	% No
Merchants	12	52%	11	48%
Banks	18	78%	5	22%
Long Distance Carriers	13	57%	10	43%

Figure 14: Revenue Realized From Partner Sources



	Yes	% Yes	No	% No
Merchant Revenue	11	48%	12	52%
Bank Revenue	16	70%	7	30%
Long Distance Carrier Revenue	12	52%	11	48%

As part of the cross-case analysis, this researcher tested the significance of partnering with merchants, banks, and long distance carriers. The hypothesis stated that partnering with merchants, banks, and long distance carriers provided revenue to the academic institution.

This researcher formulated three null hypotheses:

- Partnering with merchants does not contribute to a revenue stream;
- Partnering with financial institutions does not contribute to a revenue stream;
- Partnering with long distance telecommunication carriers does not contribute to a revenue stream.

To test the null hypotheses, this researcher utilized the chi-square test. The chi-square analysis tested the independence of each of the two variables:

- Partnering with merchants and a recognized revenue stream are independent variables;
- Partnering with financial institutions and a recognized revenue stream are independent variables;

- Partnering with long distance telecommunication carriers and a recognized revenue stream are independent variables.

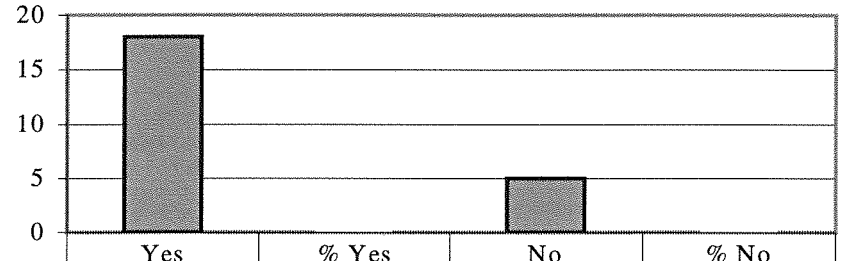
In all cases, the observed significance level of the chi-square statistic was less than .05 (.00001, .00013, .00000) (Appendixes E, F, and G). As a result, this researcher rejected each of the null hypotheses. There is evidence that each of the three sets of variables are correlated.

As evidenced, academic institutions that partner with off-campus merchants, financial institutions, and/or long distance telecommunication carriers are likely to recognize a revenue stream from these sources. However, additional testing of these variables is warranted with a larger sample size.

Case Study - Phased Implementation

Question 8 tested for the difficulty of the systems implementation phase. A total of 18 (78%) of the academic institutions stated that systems implementation was the most difficult phase (Figure 15).

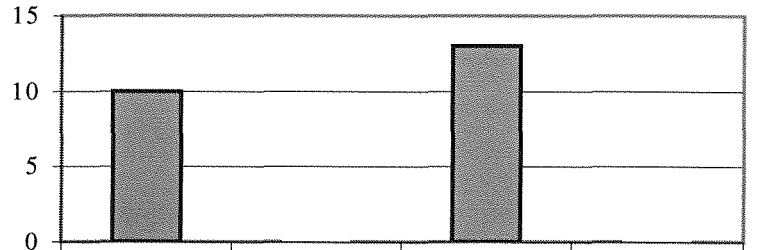
Figure 15: Implementation Phase as Most Challenging Phase



	Yes	% Yes	No	% No
Implementation	18	78%	5	22%

Question 16 tested for a phased implementation approach. The survey results indicated that 43% of the universities adopted a phased systems implementation approach; 57% did not adopt a phased approach (Figure 16).

Figure 16: Colleges Utilizing a Phased Implementation



	Yes	% Yes	No	% No
Phased Implementation	10	43%	13	57%

As part of the cross-case analysis, this researcher tested the significance of a phased implementation approach and the perceived difficulty of the implementation phase. The stated hypothesis follows:

- A phased implementation approach will reduce the perceived difficulty of the implementation stage.

This researcher formulated the null hypothesis:

- A phased implementation approach is independent of the perceived difficulty of the implementation phase.

To test the null hypothesis, this researcher utilized the chi-square test. The chi-square analysis tested the independence of each of the two variables:

- Phased implementation approach; and,
- The difficulty of the implementation phase.

The observed significance level of the chi-square statistic was less than .05 (.00395) (Appendix H). As a result, this researcher rejected the null hypothesis. There is evidence that the variables are dependent variables. However, to confirm the hypothesis, the data must be re-tested with a larger sample size.

As evidenced, academic institutions that adopt a phased systems implementation approach will likely not view the systems implementation phase as the most challenging. Additional testing of these two variables is warranted with a larger sample size.

Findings

Findings - Cross-Case Survey Analyses

The cross-case survey analyses presented significant findings and formed the basis for documenting a paradigm for the development of a university-wide smart card student identification system. As previously noted, surveys were administered to 23 of 25 colleges and universities currently utilizing smart card technology as part of their multi-application student identification card. The surveys focused on four variables:

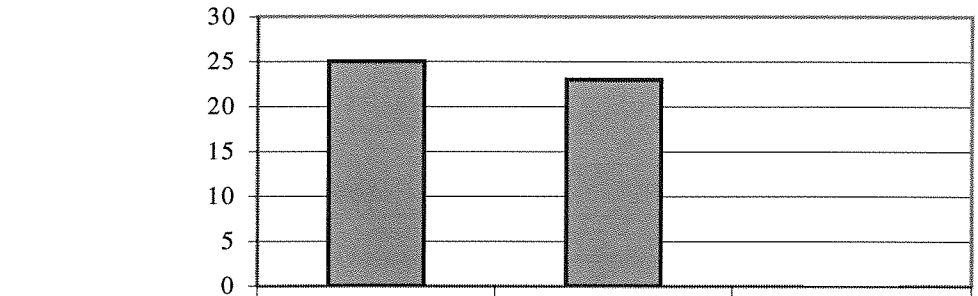
- Campus card technology;
- Managed card systems;
- Partnerships with merchants, banks, and long distance carriers; and,
- Phased systems implementations.

These four key variables will be addressed in subsequent sections. They formed the basis for a paradigm for the development of a university-wide smart card student identification system.

At the time the survey was administered, the National Association of Campus Card Users (NACCU) identified 25 academic institutions using smart card technology.

This researcher telephoned all 25 colleges and universities and requested participation in the survey. A 92% participation rate was obtained from the case study surveys (Figure 17).

Figure 17: Survey Participation Rate



	Telephoned	Participated	Participation Rate
Colleges/Universities	25	23	92%

Nova Southeastern - Campus Wide Student Identification System

Based on survey results generated by the cross-case analyses and this researcher's systems analysis presented earlier, the proposed Nova Southeastern student identification system will be a complete online, one-card, campus-wide ID card and access management system. The system will include point-of-sale, food services and meal plans, prepaid services and credit accounts, and door/building access control. Additionally, the system will support access to and use of photocopy, vending, and laundry machines and support campus bookstore purchases. The system will support video imaging ID card production. Future enhancement considerations to the system will explore the secure access to student records and transcripts.

As alluded to in Chapter 3 by the TOLIMAC project, Smart cards offer significant potential in terms of NSU's library requirements. The partnership between NSU and the

Broward County Public Library system requires librarians to distinguish between NSU students and Broward County residents. A smart card-based system enables the library to control access to specific services, modulate access and charges according to user profiles, provide an e-purse for financial transactions, and regulate Internet access.

Based on the results documented in the Survey Analysis section, subsequent sections will address the development of a paradigm for a university-wide smart card student identification system. Four areas will be addressed:

- Combination card technology;
- Managed card systems;
- Partnering with merchants, banks, and long distance carriers; and
- Phased implementations.

Findings - Combination Card Technology

As evidenced by the cross-case survey results, each of the 23 campus cards utilized various technologies to provide a multiplicity of services. Examples included:

- The color photograph and signature allowed for greater security;
- A magnetic bank-strip linked the card to a bank account for use as a debit card and ATM card;
- A library number provided access to library materials;
- A smart chip provided electronic purse functions;
- A telephone calling card number provided long distance service with competitive rates.

The proposed scope of the Nova Southeastern campus identification card as well as the proposed technologies for each service are referenced below (Table 10).

Table 10: Potential Scope of ID Card Services and the Proposed Technologies

	NSU on-line	Bank on-line	Off-Line	Technology
COMPUTING				
Printer fees			X	Smart chip
Access control	X			Magnetic strip
Network Charges		X		Magnetic strip
HOUSING/FOOD SVC				
Meal Plan/Dining access	X			Magnetic strip
Residence hall access	X			Magnetic strip
Vending			X	Smart chip
Laundry service			X	Smart chip
FINANCIAL AID				
Electronic applications	X			Magnetic strip
Electronic payments		X		Magnetic strip
COMMERCIAL USAGE				
Long distance phone			X	Access Number
Banking		X		Magnetic strip
Debit card		X		Magnetic strip
ATM services		X		Magnetic strip
Point of Sale (POS)	X			Magnetic strip
Off-campus merchants		X		Smart chip
On-campus merchants		X		Smart chip
LIBRARY				
Book checkout	X			Access Number
Fine billing		X		Smart chip
Copy service		X		Smart chip
POLICE SERVICES				
Parking	X			Magnetic strip
Fine/fee payments		X		Smart chip
REGISTRAR				
Address update	X			Magnetic strip
Phone registration	X			Magnetic strip
Lab access	X			Magnetic strip
Self Inquiry	X			Magnetic strip

Findings - Managed Card Systems

As indicated by the survey results, 96% (22) of the campus-wide systems are managed card systems. In managed card systems, the academic institution establishes a mutually-beneficial business partnership with a vendor. The vendor is the comprehensive source for all products, services and components for a complete and comprehensive multi-application campus card system. In addition to the design, development and implementation of the system, the vendor provides ongoing opportunities to expand and enhance the system.

Based on the survey results generated by the cross-case analyses and this investigator's research, the decision was made to select Cybermark to manage the design, development, implementation and ongoing management of the Nova Southeastern university-wide smart card student identification system.

As of November, 1999, Cybermark installed 20 campus smart card systems across the United States. The company's expertise in campus smart cards can be attributed to the current vice president, Bill Norwood. Prior to Cybermark's formation, Norwood orchestrated the multi-function campus smart card system at Florida State University in the mid-1990s (Cybermark, 1999).

All Cybermark smart cards incorporate both magnetic strip and microprocessor chip technology. Additionally, Cybermark focuses on implementing smart card technology while maintaining the existing infrastructure, including meal plans and university databases. The Cybermark system ensures integration with the Nova Southeastern current meal plan system. The University's meal plan system was recently upgraded to comply with Year 2000 standards.

Although the survey results indicated smart chips are used for electronic purse functions only, Cybermark provides additional uses for microprocessor chip technology. According to Cybermark (1999) these include:

- Network security. With a smart card, the institution can restrict access to campus personal computers (PC) and secure data on those PCs;
- Student voting. Smart card-based voting automates, streamlines, and secures student elections. The application utilizes both off-line terminals and Internet-based voting at campus PCs. The security of the smart card ensures that only eligible cardholders are able to vote while prohibiting duplicate voting;
- Resource tracking. The smart card documents the length of time spent in counseling sessions, tracks hours spent in computer labs, or logs attendance in vocational programs. Automating these processes improves data collection and evaluation of resource utilization.

An important benefit of a managed card system, is the ability of the vendor to link the campus card program with partnering companies. These strategic partnerships with merchants, banks, and long distance carriers contribute to the success of a campus card system and are discussed in more depth in the next section.

Findings - Partnerships With Merchants, Banks, and Long Distance Carriers

Partnerships are key to the campus smart card program. More specifically, the formation of major strategic partnerships prior to the launch of the campus smart card system are essential.

As evidenced by the survey results, the formation of partnerships with merchants, banks, and long distance carriers provided a revenue stream to the university. For

example, when the university forms a partnership with a bank, the bank does not have to issue its own cards to students; the university is in receipt of a steady stream of revenue. The bank will normally pay a fixed amount to the university each month based on the number of ATM transactions. The university may also receive income based on the average balance held in a campus card-linked bank account. Additionally, the campus card also doubles as a telephony calling card and offers students favorable rates for long distance telephone calls. In these cases, the university may expect a revenue income stream based on cardholder usage.

For many universities, the generation of revenue streams is essential to fund a smart card system rollout. For example, one of the universities interviewed is receiving funding from the regional transit authority to add a contactless chip to its ID card so students can use the card to pay for rides on trains and buses.

Universities also charge merchants' transaction fees for purchases initiated with the campus card at on- and off-campus locations. The fees are an essential vehicle for recovering system implementation costs.

Universities with successful campus smart card programs have pursued as many income streams as possible to assist in funding the card. These universities have recognized cost recovery and are managing systems that are fully costed and self-supporting.

Findings - Phased Implementations

According to survey results previously presented, 18 (78%) of the academic institutions viewed the implementation phase as the most challenging. Additionally, 13 (57%) of the academic institutions had not utilized a phased implementation approach.

However, the institutions that utilized a phased implementation did not view the implementation phase as the most difficult task (Table 11).

Table 11: Universities Using Phased Implementation

College	*Implementation Viewed as Most Difficult Phase*	*Phased Implemention Utilized*	*Vendor*
U1	Yes	No	AT&T
U2	Yes	No	AT&T
U3	Yes	No	AT&T
U4	**No**	**Yes**	**Cybermark**
U5	Yes	No	Pioneer
U6	Yes	Yes	Schlumberger
U7	Yes	No	Cybermark
U8	Yes	No	NCacheCard
U9	Yes	Yes	Gen'l Meters
U10	Yes	No	Schlumberger
U11	Yes	No	AT&T
U12	Yes	No	Cybermark
U13	**No**	**Yes**	**Cybermark**
U14	Yes	Yes	Cybermark
U15	Yes	No	Cybermark
U16	Yes	Yes	Cybermark
U17	Yes	No	Cybermark
U18	Yes	No	Cybermark
U19	Yes	Yes	Cybermark
U20	**No**	**Yes**	**Cybermark**
U21	**No**	**Yes**	**Cybermark**
U22	**No**	**Yes**	**Cybermark**
U23	Yes	No	Cybermark

As described by Whitten et al. (1994), a phased or staged conversion strategy is based on the concept of implementing successive versions of the system as each is developed. A phased implementation approach enables Nova Southeastern University to concentrate on those opportunities that rank high in priority and urgency (Table 12).

Table 12: Problem Statements

Brief statement of problem, opportunity, or directive	Urgency	Visibility	Priority or Rank	Proposed Solution
1. The university's declining balance meal plan system is a DOS-based system that is non-compliant for use in the year 2000	**ASAP**	**High**	**1**	**Quick fix; then new development**
2. NSU does not utilize a multi-application student campus card, but utilizes separate cards for campus functions	6 months	Med	2	New Development
3. The challenge for NSU is to offer an access card that will differentiate NSU students from Broward county residents utilizing the new technology center	**3 months**	**High**	**1**	**New Development**
4. NSU multi-card applications are not well integrated to maximize efficiency and convenience for students, faculty and staff	6 months	Med	2	New Development

By implementing multi-function student identification cards with smart card technology, Nova Southeastern University can:

- Provide a single, recognizable university identification card;
- Utilize a single, integrated identification card production system with multi-campus on-site photo capture and production capability;
- Integrate the new card with current university applications such as meal-plan, library, access control; and
- Offer new card-based services such as banking, long distance telephony and vending (on- and off-campus points of sale).

Moreover, Nova Southeastern can also:

- Provide a single, convenient method to access campus services;
- Provide a point-of-sale (POS) debit card for use at off-campus merchants;
- Increase the effectiveness of campus-based systems by promoting one card access;
- Expand the current system to integrate with other information systems on campus; and
- Establish a technological infrastructure for accommodating current needs and future requirements.

It is important to note that the paradigm for a university-wide smart card student identification system can be adopted by other academic institutions.

Summary of Results

This chapter presents survey results and cross-case analyses associated with the population of academic institutions utilizing smart card technology as part of their campus student identification card system. Based on the statistical findings, a plan for the development and implementation of a university-wide smart card student identification system was presented. The outline illustrates an implementation model specifically designed for Nova Southeastern University.

The paradigm for a university-wide smart card student identification system featured four key points:

- Card technology, including magnetic strip and smart chip;
- Managed card systems;
- Strategic partnerships with merchants, banks, and long distance carriers; and
- Phased or staged system implementations.

Statistical findings identified similarities between each of the case studies. These similarities, in concert with statistical analyses, were utilized to develop the paradigm for a university-wide smart card student identification system.

Chapter V

Conclusions, Implications, Recommendations, and Summary

Conclusions

This dissertation investigation documents a model for the design and development of a university-wide smart card student identification system. The proposed model is based on an analysis of 23 colleges and universities currently utilizing smart card technology as part of their campus card systems. In this multiple-case study, the goal was to build a general explanation that fit each of the individual cases, even though the cases varied in their details. The general explanation is a documented paradigm for the development and implementation of a smart card system in a university environment. The university environment on which the paradigm is based is Nova Southeastern University (NSU), located in Fort Lauderdale, Florida. The paradigm specifically answered the question:

- How can NSU effectively implement a smartcard system to optimize the use of multiple application card access?

The paradigm is distinguished by the following key elements:

1. *The campus card combines magnetic strip and smart chip technology.* The key emphasis is on one card providing a multiplicity of services and functions. This is accomplished by utilizing different technologies on the same card. Campus cards can perform different types of transactions and, therefore, require different technologies.

Debit transactions and ATM transactions are drawn directly from a checking and/or savings account. These transactions typically utilize magnetic strip technology and operate in an online mode. In contrast, recent smart card technology allows a user to load funds directly onto the smart chip. The card operates in an off-line mode and is used in the place of cash in vending machines, college bookstores, photocopying machines and dormitory laundry rooms.

2. *The campus card system is a managed card system.* The concept of managed card systems prevailed throughout the cross-case analyses. As part of the paradigm developed in this dissertation investigation, Cybermark was chosen as the vendor of choice. As of November, 1999, Cybermark installed 20 campus smart card systems across the United States. Cybermark focuses on implementing smart card technology while maintaining existing infrastructure, including meal plans and university databases. An important benefit of a managed card system is the ability of the vendor to link the campus card program with partnering companies.
3. *The campus card system includes strategic partnerships with merchants, banks, and long distance carriers.* The formation of major strategic partnerships prior to the launch of the campus smart card system is essential. As evidenced by the survey results, the formation of partnerships with merchants, banks and long distance carriers provided a revenue stream to the university. Universities with successful campus smart card programs pursued as many income streams as possible to assist in funding the card. These universities recognized cost recovery and are managing systems that are fully costed and self-supporting.

4. *Systems implementation is phased or staged.* As described by Whitten et al. (1994), a phased or staged conversion strategy is based on the concept of implementing successive versions of the system as each is developed. A phased implementation approach enables Nova Southeastern University to concentrate on those opportunities that rank high in priority and urgency.

NSU can recognize the following benefits from the implementation of a multiple application smart card system:

- The university will have a single, unified student identification and financial transaction card;
- The card will provide a single, convenient method to access on-campus services;
- The card will increase the effectiveness of campus-based systems by promoting a one-card access to services;
- The university will recognize cost savings by combining its many campus cards into one centralized card; and
- The university will receive revenue from the formation of strategic partnerships with merchants, banks, and long distance carriers.

Implications

This dissertation featured the development of a paradigm for a university-wide smart card student identification system. This paradigm is based on statistical analysis and a multiple-case study of academic institutions currently utilizing smart card technology in their campus card programs. However, the use of smart card technology on the university campus is still in its infancy. Its ramifications and opportunities are still unknown and numerous applications are not yet identified or defined. As additional

applications are identified and understood, these should be integrated into future paradigms.

Future Research

The use of smart card technology presents a new range of opportunities. Current projects and pilot programs in the field of smart card technology can serve as a basis for future research. Examples of these projects include the Electronic Trading Organization (ETO) smart card, the DISTINCT project, and the SCARAB project.

The ETO Authentication Smart Card

The ETO (Electronic Trading Organization) was developed by the United Nations Trade Point Development Center (UNTPDC). The ETO system provides subscribers around the world with a single point of contact for trade, investment and business opportunities using an international standard called the Global Trade Point Network (ETO, 1999). The ETO system currently connects 135 Trade Points and 10,000 related bodies in 75 developed countries, 60 developing countries and 20 less developed countries (ETO, 1999). According to the ETO (1999), the removal of trade barriers in many countries has prompted the need for the ETO to collect, process and disseminate fast and accurate commercial information using electronic commerce technologies.

The ETO is currently testing smart cards as an efficient and secure method of storing and transferring information. The ETO smart card ensures that cardholders' information is secured as it travels across the Global Trade Point Network (GTPNet). Confidentiality is ensured by the use of message encryption on both the card and on the ETO Master Web Index (ETO, 1999). The goal of the ETO Smart Card Project is to

enable ETO members to pay for goods and services over the GTPNet and Internet using an ETO issued smart card and personal computer.

DISTINCT Project

The DISTINCT Project is a two-year project funded by the European Union (EU). The project began in February 1998 and will end in January 2000 (Smartcard Club, 1999). DISTINCT stands for Deployment and Integration of Smartcard Technology and Information Networks for Cross-sector Telematics. The project currently has five demonstration sites: Torino, Italy; Thessaloniki Greece; Lapland, Finland; Newcastle, United Kingdom; and Zeeland, The Netherlands.

The goal of the project is to implement and integrate smart card applications that span sectors, such as healthcare, transportation, citizen services, and libraries (The Smartcard Club, 1999). Integration will take place using an application program interface (API) called a DISTINCT ID. A DISTINCT ID is a set of data that resides on the card and allows interoperability (The Smartcard Club, 1999). Additionally, the DISTINCT ID supports application integration within a site or region regardless of whether single application or multi-application cards are used or the card types used.

Smart Card and Agent Enabled Reliable Access (SCARAB)

The ACTS Program was established under the Fourth Framework Program of European activities in the field of research and technological development. The SCARAB project, funded by the ACTS Program, is evaluating the use of smart cards as universal tokens for seamless access to telecommunications services in an open architecture (Infowin, 1999). The goal of the project is to increase the awareness of the capabilities of smart cards as personal identification and authentication devices.

Additionally, the project's objective is to address the standardization of smart cards for use across heterogeneous infrastructures (Infowin, 1999).

Security - An Important Consideration

Given the appropriate time and resources, any system can be compromised (Krueger & Schloss, 1998). However, a smart card is an intrinsically secure device. According to Krueger and Schloss (1998), attacks on smart card systems can be classified as Class 3 attacks, which means it takes millions of dollars of sophisticated equipment to break into a smart card transaction. However, in September, 1999, the Smart Card Forum announced that its strategic direction for the year 2000 will include a new work group focused on the application of smart cards, public key infrastructure (PKI), and other ID and authentication related technologies (The Smart Card Forum, 1999). The Smart Card Forum expects that the formation of its ID and Authentication Work Group will help its member organizations discover new business applications for smart card systems that enable secure electronic commerce (Smart Card Forum, 1999).

Smart card security begins with the hardware, or chip, embedded in the card and the software which controls the movement of value between cards. According to Guthery and Jurgensen (1998), the packaging of the integrated circuit chip into a smart card is typically viewed as being tamper-resistant as well as tamper apparent. Although it is not impossible to extract information from the circuit chip, it is difficult. To extract information directly from a chip requires physical possession of the card, costly equipment, and a detailed knowledge of both the hardware architecture of the circuit chip and the software loaded onto the chip.

Authentication software remotely verifies the identity of the cardholder. Examples of these protocols include Value Transfer Protocol (VTP), Public Key Infrastructure (PKI), and Secure Electronic Transaction (SET). These protocols and technologies are briefly described below.

Value Transfer Protocol (VTP)

Every Mondex smart card utilizes Value Transfer Protocol (VTP). The VTP software application sends messages between two Mondex smart cards. Utilizing sophisticated software, VTP ensures a secure and legitimate transfer from one card to another (Mondex, 1999). According to Mondex (1999), the VTP transaction occurs in two steps. First, the two cards validate each other. Secondly, the cards utilize digital signatures to authenticate messages and transfer the value.

According to Mondex (1999), the transaction between a consumer and merchant happens in a matter of seconds:

- Information from the consumer's chip is validated by the merchant's chip. Similarly, the merchant's card is validated by the consumer's card;
- The merchant's card requests payment and transmits a digital signature with the request. Both cards check the authenticity of each other's message. The customer's card checks the digital signature and, if satisfied, sends acknowledgement, again with a digital signature;
- Only after the purchase amount has been deducted from the consumer's card is the value added to the merchant's card. The digital signature from this card is checked by the consumer's card and, if confirmed, the transaction is complete.

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) smart cards enable secure remote authentication by utilizing a cryptoprocessor handling asymmetric encryption (id2tech, 1999). PKI uses an asymmetrical pair of keys: a public key and private key. The private key is stored within the smart card and encrypts information that can only be deciphered by the corresponding public key (Eriksoo, 1999). The private encryption key is not sent over the Internet with the transaction, but remains encoded in the smart card. This makes the system difficult for hackers to break the security scheme.

According to Eriksoo (1999), a secure, remote authentication takes a matter of seconds to complete:

- The client takes up the connection with the merchant's server;
- The merchant's server sends an identification question;
- The client transmits the question to the smart card;
- With the help of encoding, the smart card creates a digital signature for the question. This key cannot be altered by viruses or broken into because the encoding is not processed by the computer, but by the card itself;
- The smart card sends the signed question back to the client;
- The client sends the answer to the question back to the merchant's server; and
- The merchant's server controls the validity of the signature and allows access after correct identification.

Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET), developed by Visa and MasterCard, is a technical specification for securing payment-card transactions over open networks such as the Internet (Visa SET Protocol, 1999). SET utilizes digital certificates to authenticate the cardholder and merchant. The cardholder's digital certificate contains information about the account, the financial institution, and some cryptography information (Visa SET Protocol, 1999). The merchant's digital certificate contains information about the merchant, the merchant's financial institution and the financial institution issuing the certificate (Visa SET Protocol, 1999).

According to Visa Card Services (1999), there are five elements to SET:

- A certificate authority that issues digital certificates of authenticity to cardholders and merchants;
- Cardholder software is kept in each individual's personal computer. This software stores and maintains the digital certificate and encrypts messages;
- Merchant software that manages their digital certificate and interfaces with the acquiring bank; and
- A payment gateway utilized by the acquiring financial institutions to process and decrypt the transaction when it arrives from the merchant and re-encrypt information returned to the merchant.

The SET process involves exchanging coded information between the consumer, the merchant, a Payment Gateway, and both the consumer's card issuer and the card processing institution. The information is coded using public and private keys. The

information is encoded using a public key; only the holder of the appropriate private key can decode the information.

According to Visa Card Services (1999), SET offers a very high level of security. SET implementation involves the following process:

- A consumer's order is sent to the merchant;
- The consumer's request to make a payment is sent to the merchant's credit card processor;
- Both the identity of the consumer and the merchant are confirmed;
- The merchant receives a payment authorization and the consumer receives a receipt; and
- The merchant never sees the consumer's credit card number and the payment authorization the merchant receives is for a single transaction and cannot be used again.

According to Eriksoo (1999), the lack of user confidence in the security of online transactions is surprising considering the technology is tried, tested, and currently used in the financial marketplace. Internet services must guarantee the highest standards of security and take the necessary measures to increase consumer and business users' confidence in the Internet and Internet security.

Nova Southeastern Smart Card System

If NSU adopts the paradigm described in this dissertation and implements a smart card student identification system, additional data should be continuously collected as a basis for further smart card system enhancement. More specifically, additional data

regarding the NSU smart card student identification system can be captured, monitored, and compared with other universities utilizing smart card technology.

Current research illustrated by projects such as the Electronic Trading Organization (ETO) smart card, the DISTINCT initiative, and the SCARAB implementation can serve as a framework for future research for the Nova Southeastern campus smart card system. The results of this research can impact the functionality of future smart card systems in other academic institutions as well.

Various considerations must be addressed before implementing smart card technology. Because smart cards are not PIN-protected, the value stored on the card can be used by anyone (Berger, 1997). For this reason, institutions such as Florida State University, Pennsylvania State University and University of Michigan limit the amount of funds that can be stored on the smart chip.

Secondly, strategic partnerships are a key element of campus smart card systems. Academic institutions such as Middlebury College, Kansas State University, and Villanova University enter into partnerships with financial institutions. These agreements traditionally are established with a single bank. If cardholders wish to utilize the banking features of the card, their deposits must be held by the preferred financial institution. Approximately 73% of all students enrolled at NSU report Florida as their permanent residence (Nova Southeastern University Fact Book, 1999). Therefore, an established relationship between NSU and a Florida-based bank is sufficient.

At the time of this dissertation investigation, 25 of the 3,500 (.7%) colleges and universities implemented smart card technology as part of their campus card system. The data for formulating this paradigm was captured from 23 of the 25 academic institutions

currently utilizing smart card technology. This number represents 92% of the population. However, this number is too small to represent a statistically significant sample. As additional universities adopt smart card technology, it is recommended that the paradigm be enhanced and changed as needed.

Recommendations

This section provides recommended guidelines regarding the systems implementation process and support activities for NSUs campus-wide smart card student identification system. This section addresses phases three and four of the Whitten et al. (1994) Modern Systems Development Life Cycle (MSDLC) model.

Systems Design

According to Whitten et al. (1994), systems design builds on the knowledge obtained from systems planning and systems analysis. Systems design involves phases:

- Selection of a design target;
- Acquisition of necessary hardware and software; and
- Design and integration of the new system.

Select a Design Target

The first phase of systems design is to identify and select a feasible design solution. For the purposes of this dissertation investigation, a campus-wide smart card student identification system solution is defined and described. The proposed Nova Southeastern student identification system is a complete online, one-card, campus-wide ID card and access management system. The system includes point-of-sale, food services and meal plans, prepaid services and credit accounts and building access control. Additionally, the system can be used in vending and laundry machines and facilitate

campus bookstore purchases. The system supports video imaging ID card production. Future enhancement considerations to the system will explore the secure access to student records and transcripts.

The smart card offers significant potential in terms of NSU's library requirements. A total library management system such as the TOLIMAC project described earlier, enables NSU to define a policy for accessing services. A total library management concept ensures NSU to differentiate NSU students from Broward county residents utilizing the new Library, Research and Information Technology Center. Additionally, smart card technology enables users to access a range of services using a single card.

A total library management system integrates management and control of information resources and associated costs. A requirement of the NSU Library, Research and Information Technology Center is the ability to allocate costs to the Broward County Library System. Smart card technology, as utilized in the TOLIMAC system, enables NSU to allocate service costs to the Broward County Library System.

Access to resources is controlled by means of a personal smart card issued to a registered library user (Information Society Technologies, 2000). The smart card profile restricts access to selected services and specifies the cost of the services. The system monitors services used. This is accomplished by the authentication process which supports cost allocation (Information Society Technologies, 2000). For example, the system will monitor electronic document delivery to an individual user. Costs for the delivery service are allocated accordingly.

Importantly, the smart card is a local card for use on the NSU campus. In addition to library services, the card is used for various campus services including photocopying, building access and vending services.

Acquire Necessary Hardware and Software

It is recommended that all applications supported by the smart card system utilize the same single, central databases; the same software; and, the same card reader family. Implementation of multiple integrated systems that utilize multiple integrated databases from multiple vendors is a barrier to effective use.

The hardware and software contributing to the framework of the smart card system should reflect the following guidelines:

- ID cards should use a standard American Banking Association (ABA) magnetic strip and encoding techniques;
- ID cards should follow specific International Standards Organization (ISO) and American National Standards Institute (ANSI) guidelines;
- Card system software should have the ability to reconcile the balances of credit/debit accounts with the balance of all reader transactions for a specified date; and
- ID system software should support multiple identifier numbers such as Social Security Number (SSN), ISO, ANSI, and American Banking Association numbers.

Design and Integrate the New System

As recommended earlier, the solution developed by Cybermark is the system of choice to implement the NSU smart card student identification system. This recommendation is made based on this investigator's research and Cybermark's ability to

integrate the smart card system with existing meal plans; security and access systems; library software; and university databases.

Systems Implementation

The systems implementation phase consists of four phases:

- Build and test networks and databases;
- Build and test the program;
- Install and test the new system; and
- Deliver the new system.

Build and Test Networks and Databases

According to Whitten et al. (1994), in many cases, new or enhanced applications are built around existing networks and databases. In these cases, this phase can be omitted. In terms of NSU's campus-wide smart card student identification system, existing networks and databases are utilized. Therefore, this phase is not necessary.

Build and Test the Programs

According to Whitten et al. (1994), the fundamental objectives of this phase include developing and testing computer programs that fulfill business process requirements. Additionally, Whitten et al. (1994) state that this phase is necessary only if the computer programs are developed in-house. For NSUs campus-wide smart card student identification system, the required software is provided by Cybermark. Therefore, this phase is not necessary.

Delivering the New System Into Operation

This is the last phase of systems implementation. This phase ensures a smooth transition from the old system to the new system. As indicated in the paradigm, it is

recommended that NSU carry out a phased or staged system conversion. A staged conversion can facilitate a smooth transition to the new system.

This phase involves the issuance of student identification cards. It is recommended that Cybermark orchestrate the mass card issuance. This ensures that students receive the smart cards quickly and efficiently. In addition, Cybermark should also be responsible for the necessary staff and equipment to ensure that the smart card systems are implemented reliably and dependably.

Importantly, this phase includes training end-users and evaluating the project and the final system. A systems audit identifies techniques for systems improvement. The feedback received from the systems audit phase is critical. This data contributes to the effectiveness of the implementation phase and integration of successive applications. Adequately marketing the campus-wide student identification system and training and educating the NSU community are indispensable in achieving a successful implementation of the multi-application smart card system.

Summary

This dissertation investigation documents a paradigm for the development of a university-wide smart card student identification system. The model is specifically designed to be utilized by Nova Southeastern University, in Fort Lauderdale, Florida. This proposed paradigm represents a realistic model that can be institutionalized by other colleges and universities.

Currently, NSU utilizes a traditional photo ID card system that enables students, faculty, and staff to borrow books and materials from NSU libraries. A second card is

issued to students participating in the university meal plan. Additionally, the university also issues separate declining balance cards for utilizing library photocopiers.

Nova Southeastern University administrators from Business Services, Library Services, and Food Services envision a single, unified identification and transaction card system that supports multiple functions. The card can increase effectiveness of campus-based systems by promoting card-based access to services. Finally, the card is a reliable mechanism for ensuring that the cardholder is currently registered or employed by the University and therefore is eligible to access and receive university services.

The paradigm for the development of a university-wide smart card student identification system for members of the NSU community is based on the statistical analysis of data collected from academic institutions currently utilizing smart card technology. The systems planning phase for this dissertation investigation documents a smart card paradigm in terms of NSU's mission, goals, objectives and requirements.

The procedures for implementing the paradigm are based on the Modern Systems Development Life Cycle (MSDLC) model developed by Whitten et al. (1994). Additionally, case study procedures developed by Yin (1994) serve as the framework for analyzing case study data collected from colleges and universities utilizing smart card technology.

This dissertation investigation involves an extensive examination of multi-application campus card technology, including smart card technology. If implemented at NSU, a multi-application campus smart card can:

- Provide a single, recognizable University ID card;

- Integrate the new card with current University applications such as meal-plan, library and access control; and
- Offer new card based services such as banking, long-distance telephony and vending.

Importantly, a multi-application campus smart card provides a range of applications such as network security, campus security and storage of student information. The card is a flexible tool for accommodating current and future NSU requirements. Additionally, the campus smart card enables NSU to take a leadership role in utilizing this technology.

It is important to note that this dissertation inquiry is based on interviewing key personnel at colleges currently utilizing smart card technology. As a consequence, only 23 of 3,500 colleges and universities participated in this study. Nonetheless, the paradigm for the design, development, and implementation of a multi-functional smart card information system represents important procedures and techniques for effective implementation and ongoing assessment. The smart card implementation process is clearly established. The paradigm is subject to change as a consequence of innovations in the technological domain. Therefore, the smart card information system paradigm should be regularly reviewed and revised to reflect technological advancements.

Appendix A

Campus Card Survey

1. How many smart applications is the college currently utilizing on campus? CHECK ALL THAT APPLY

(a) Vending	Yes	No
(b) Copiers	Yes	No
(c) Printers	Yes	No
(d) Meal Plan	Yes	No
(e) Book Store	Yes	No
(f) Library Access	Yes	No
(g) Credit/Debit Card	Yes	No
(h) Pre-deposit value management/Electronic Purse	Yes	No
(i) Laundry	Yes	No
(j) Security/Access Control	Yes	No
(k) Parking	Yes	No
(l) Time Management	Yes	No
(m) Off campus point-of-sale	Yes	No
(n) Financial Institutions	Yes	No
(o) Video Imaging System	Yes	No
(p) Telecommunications-Long distance service	Yes	No
(q) Financial Aid Distribution	Yes	No
(r) Student Payroll	Yes	No
(s) Student Identification	Yes	No
(t) Class Registration	Yes	No

2. Is the college utilizing smart card technology? Yes No

   Is the college utilizing magnetic strip technology? Yes No

3. What is the name of the provider of the platform on which the card system operates? PLEASE CHECK ONLY WHAT APPLIES.

(a) Atlantek Inc.	Yes	No
(b) Advances Polymer Associates	Yes	No
(c) American Card Technology	Yes	No
(d) AT&T Campus Wide Solutions/Harco Inc.	Yes	No
(e) BTS Enterprises	Yes	No
(f) Capcard	Yes	No
(g) Casi Rusco	Yes	No
(h) The Cboard Group Inc.	Yes	No
(i) Cybermark	Yes	No
(j) General Meters	Yes	No
(k) GTE Network Services	Yes	No
(l) Image Data Systems, Inc.	Yes	No
(m) Security One Systems	Yes	No
(n) Sensormatic Electronics Corp.	Yes	No
(o) IBM Inc.	Yes	No
(p) NPD & Associates	Yes	No
(q) Cardtech	Yes	No
(r) Special Teams/College Enterprises Inc.	Yes	No

4. Is there technical documentation available that details the technical architecture of the system? Yes No

5. What technical challenges were presented during design and implementation? PLEASE CHECK ONLY WHAT APPLIES.

(a) Software	Yes	No
(b) Hardware	Yes	No
(c) Video Imaging	Yes	No
(d) Network	Yes	No
(e) Intranet Access	Yes	No

6. Which department/office was given the responsibility for the development of the project and eventual administration of the system? PLEASE CHECK ALL THAT APPLY.

(a) Business Services	Yes	No
(b) Public Safety	Yes	No
(c) Registration Office	Yes	No
(d) Admissions	Yes	No
(e) OIT	Yes	No
(f) Bursar's Office	Yes	No

7. What benefits has the university recognized by utilizing Smart Card technology?

(a) Revenue Source	Yes	No
(b) Safety of persons and property	Yes	No
(c) Cost savings	Yes	No

8. Which phase of the process was the most challenging?

(a) Design	Yes	No
(b) Development	Yes	No
(c) Implementation	Yes	No

9. Have you partnered with any local merchants? Yes No

10. If yes, what level of participation?

1-10 merchants	Yes	No
11-20 merchants	Yes	No
Above 20 merchants	Yes	No

11. Is there a revenue stream associated with any of these merchants? Yes No

12. Have you partnered with a financial institution that offers additional services to students? Yes No

    (a) Checking Yes No
    (b) Savings Yes No
    (c) Visa/Mastercard Yes No

13. Is there a revenue stream associated with any of these Institutions? Yes No

14. Have you partnered with any long-distance carriers? Yes No

15. What level of participation?

    (a) Calling card Yes No
    (b) Discounted rates Yes No

16. Was the system implementation accomplished in phases? Yes No

Appendix B

Chi-Square Test
Variables: Cybermark and Revenue

SYS	Count	REV No .00	REV Yes 1.00	
	Cybermark	1	13	14 60.9
	Other	1	8	9 39.1
	Column Total	2 8.7	21 91.3	23 100

Chi-Square	Value	DF	Significance
Pearson	.10865	1	.74168
Continuity Correction	.00000	1	1.00000
Likelihood Ratio	.10630	1	.74439

Minimum Expected Frequency	.783
Cells with Expected Frequency < 5	2 OF 4 (50%)

Appendix C

Chi-Square Test
Variables: Cybermark and Safety

SYS	Count	SAF No .00	Yes 1.00	
	Cybermark		14	14 60.9
	Other	3	6	9 39.1
	Column Total	3 13.0	20 87.0	23 100

Chi-Square	Value	DF	Significance
Pearson	5.36667	1	.02053
Continuity Correction	2.83013	1	.09251
Likelihood Ratio	6.35451	1	.01171

Minimum Expected Frequency	1.174
Cells with Expected Frequency < 5	2 OF 4 (50%)

Appendix D

Chi-Square Test
Variables: Cybermark and Savings

SYS	Count	SAV No .00	SAV Yes 1.00	
	Cybermark	3	11	14 60.9
	Other	6	3	9 39.1
	Column Total	9 39.1	14 60.9	23 100

Chi-Square	Value	DF	Significance
Pearson	4.70692	1	.03004
Continuity Correction	2.99923	1	.08330
Likelihood Ratio	4.78359	1	.02873
Minimum Expected Frequency	3.522		
Cells with Expected Frequency < 5	1 OF 4 (25%)		

Appendix E

Chi-Square Test
Variables: Partnering with Merchants and a Recognized Revenue Stream

MERCH	Count	MERCH REV No .00	Yes 1.00	
NO	.00	11		11 47.8
YES	1.00	1	11	12 52.2
	Column Total	12 52.2	11 47.8	23 100

Chi-Square	Value	DF	Significance
Pearson	19.32639	1	.00001
Continuity Correction	15.82735	1	.00007
Likelihood Ratio	24.95721	1	.00000

Minimum Expected Frequency	5.261
Number of Missing Observations	0

Appendix F

Chi-Square Test
Variables: Partnering with Financial Institutions and a Recognized Revenue Stream

FINAN	Count	FINAN REV No .00	Yes 1.00	
NO	.00	5		5 21.7
YES	1.00	2	16	18 78.3
	Column Total	7 30.4	16 69.6	23 100

Chi-Square	Value	DF	Significance
Pearson	14.60318	1	.00013
Continuity Correction	10.70652	1	.00107
Likelihood Ratio	15.70920	1	.00007

Minimum Expected Frequency	1.522
Cells with Expected Frequency < 5	2 OF 4 (50%)

Appendix G

Chi-Square Test
Variables: Partnering with Long Distance Carriers and a Recognized Revenue Stream

LD	Count	LD REV No .00	Yes 1.00	
NO	.00	10		10 43.5
YES	1.00		13	13 56.5
	Column Total	10 43.5	13 56.5	23 100

Chi-Square	Value	DF	Significance
Pearson	23.00000	1	.00000
Continuity Correction	19.11075	1	.00001
Likelihood Ratio	31.49235	1	.00000

Minimum Expected Frequency	4.348
Cells with Expected Frequency < 5	1 OF 4 (25%)

Appendix H

Chi-Square Test
Variables: Phased Implementation Approach and the Perceived Difficulty of the Implementation Phase

IMPL	Count	PHASE No .00	Yes 1.00	
NO	.00		5	5 21.7
YES	1.00	13	5	18 78.3
	Column Total	13 56.5	10 43.5	23 100

Chi-Square	Value	DF	Significance
Pearson	8.305556	1	.00395
Continuity Correction	5.62665	1	.01769
Likelihood Ratio	10.22203	1	.00139
Minimum Expected Frequency	2.174		
Cells with Expected Frequency < 5	2 OF 4 (50%)		

Reference List

A rising tide of applications. (1998). *Card Marketing Top 10 Technologies Supplement, S41, S45+.*

Adams State College, (1999). *ASC/College center campus card.* http://www.adams.edu.campus_life/college_center/campus_card.htm Last modified April 8, 1999. Accessed June 13, 1999.

Alcorn, B. (1998, November 4). Smarting over smartcards. *Wired,* http://www.wired.com/news/business/story/16048.html?2. Accessed November 3, 1998. Author's email: buster@sirius.com.

Allen, C. A. & Kutler, J. (1997). Overview of smart cards and the industry. In C. A. Allen & W. J. Barr (Eds.), *Smart cards: Seizing strategic business opportunities* (pp. 2-20). Chicago, IL: Richard D. Irwin.

Balaban, D. (1999). Stepping into the spotlight. *Card Technology,* 20-24.

Balaban, D. (1999, April). The smart card as sentinel - The electronic commerce boom combined with growing concerns about the vulnerability of electronic data promises to fire interest in the use of smart cards to protect computer networks. Microsoft Corp.'s focus on chip cards for network security is fanning flames. *Card Technology,* N/A.

Bardenfleth, O. (1999, April 14). *The use of integrated circuit cards and card terminals in telecommunications.* http://www.etsi.or/ Last modified April 14, 1999. Accessed July 15, 1999.

Basch, R. (1998, February 1). Get smart or get carded. *Computer Life,*4 (2), 40-43.

Berger, A. (1997, September/October). *Campus cards get smarter.* http://www.nacs.org/info/cs/97-so/campuscard.asp Accessed December 21, 1999.

Berinato, S. (1997, March 24). Smart cards move to head of class: Florida State University embraces technology; spawns separate business to sell services. *PC Week,* 14 (13), 22.

Berinato, S. & Kerstetter, J. (1998, September 21). Smart cards get hand. *PC Week,* 15 (38), 6.

Blackburn, M. R. (1993). Smart cards in higher education. *Cardtech/Securtech 1993: Solutions for the global frontier* (pp. 691-697). Rockville, MD: Smart Card Industry Association.

Brainerd, L. & Tarbox, J. D. (1997). Healthcare and smart card technology. In C. A. Allen & W. J. Barr (Eds.), *Smart cards: Seizing strategic business opportunities* (pp. 151-168). Chicago, IL: Richard D. Irwin.

Brazel, K. (1996). *All Systems Go for Maine Motorists.* http://www.ettm.com/news/maine.html Accessed June 19, 1999.

Bull SC&T (1999). *Health cards: for a rational health system returning priority to the patient.* http://www.cp8.bull.net/products/healtha.htm Last modified April 7, 1999. Accessed June 7, 1999.

Bull and Cartes Bancaires salute 10 years of smart card fraud reduction. (1999, May 12). http://smratcardcentral.com/news/pressrelease/bull_051299_2.htm Last modified May 12, 1999. Accessed June 2, 1999.

California Institute of Technology (1998). *Caltech campus card.* http://www.caltech.edu/~cabs/card/card_off.htm Last modified March 31, 1998. Accessed June 13, 1999.

Campus ID Report (1997). *About Campus ID Report.* http://www.campusid.com/about.htm Accessed May 30, 1999. email: mail@campusid.com

CardLink (1997). *Health telematics (AIM) final report.* http://www.ehto.be/volume2/cardlink.html Last modified February 1, 1997. Accessed June 7, 1999.

Cardlogix (1998). *Smart card basics.* http://www.cardlogix.com/basics.html Accessed July 26, 1999.

CardTechnology (1999). *U.S. colleges find new revenue sources to boost smart card business case.* http://www.cardtech.faulknergray.com/stor.htm#43 Last modified April 13, 1999. Accessed June 13, 1999.

CardTrack (1997, July 2). *First Union's first college smart card.* http://www.ramresearch.com/cardtrack/news/cf7_2e_97.html Last modified July 2, 1997. Accessed July 18, 1999.

CENELEC (1998). *CENELEC Homepage.* http://www.cenelec.be/index.htm Accessed July 17, 1999.

Chiew, A., Marston, B., Brodnax, E., Huvnh, O., Sigman, R. & Lumpkin, M. (1999, June 14). *Smart cards and the dumb things they do.* http://www.cba.uga.edu/~mhaines/man564/projects/sextuplets/scard.html Last modified June 14, 1999. Accessed July 26, 1999.

Chips: Smartcards get smarter with new chips from Motorola; new chips provide the memory required for multi-application cards to become a reality, a fact not a forecast. (1998, July 6). *EDGE: Work-Group Computing Report*, 8 (23), 1.

CityU (1997). *CityU launches smart card with dual purpose.* http://www.cityu.edu.hk.mpu/linkage/03-97/ed970301.htm Last modified March 1997. Accessed August 8, 1999.

Cobb, S. (1998, April). Smartcard invasion continues. *BYTE*, 23 (4) 112c.

Coleman A. (1998, February). Giving currency to the Java Card API. *Java World.* http://www.javaworld.com/javaworld/ Last modified July 1, 1999. Accessed September 21, 1999.

Contactless smart cards in Seoul (1998). http://www.cardshow.com/guide/card/korea.html Last modified January 23, 1998. Accessed July 17, 1999.

Craig, A. (1998, March 9). *High cost of smart cards hampers adoption.* http://www.techweb.com/wire/story/TWB19980309S0025 Last modified May 31, 1999. Accessed June 26, 1999.

Cybermark (1999). *About the campus card.* http://www.cybermark.com Accessed December 21, 1999.

Davis, D. (1999, April 1). China will boosts smart cards in a big way – in its drive to modernize, China has emerged as one of the major consumers of smart cards for telecom applications. Even bigger chip card projects are on the drawing board, but full-scale roll-outs remain a few years away. *Card Technology,* N/A.

Davies, S. (1996, August 24). *Identity cards: frequently asked questions.* http://www.privacy.org/pi/activities/idcard/idcard_faq.html

Doheny, M. (1997, March 20). *Motorola smartcard systems business: Technology background.* http://www.mot.com/LMPS/pressreleases/ssbtech.html Last modified March 20, 1997. Accessed May 7, 1999.

Dorobek, C. J. (1998, August 24). GSA sets up Office of Smart Card Initiatives. *Government Computer News,* 17 (27), 7.

Dreifus, H. & Monk, J. T. (1998). *Smart cards: A guide to building and managing smart card applications.* New York: John Wiley & Sons, Inc.

du Castel, B. (1999, May). *Smart card phone home.* http://smartcardcentral.com/technical/TechTalk/column4.html Last modified May, 1999. Accessed May 30, 1999.

Engelbrecht, R. (1997, October). How to implement smart cards in health care: Experiences from pilot studies. *Toward and Electronic Health Record Europe Conference Proceedings* (pp. 45-51). Newton, MA: Medical Record Insitute.

Eriksoo, R. (1999). *Be smart, think smart cards.* http://www.id2tech.com Accessed December 21, 1999

ETO (1999). *The Secure ETO Smart Card.* http://www.eto.untpdc.org/index.html Accessed December 21, 1999.

Europay (1998). *Smart cards: EMV standards.* http://www.europay.com/SmartCard/html/Smartcard_emv.html Last modified November 11, 1998. Accessed August 2, 1999.

Europay (1999). *First interoperable EMV-chip implementation facilitated by Europay.* http://www.europay.com Last modified June 10, 1999. Accessed August 2, 1999.

Fancher, C. H. (1997, February). In your pocket smartcards. *IEEE Spectrum*, 34 47-53.

Farrell, J. J. (1996). Smartcards become an international technology. *Tron Project International Symposium* (pp. 134-140). IEEE Computer Society Press.

Flohr, U. (1998, January). Smartcards, ubiquitous in Europe, are set to hit the United States at last. *BYTE*, 23 (1), 76.

Florida Department of Transportation (1999). *SunPass Electronic Toll Collection.* http://www.sunpass.com Accessed June 19, 1999.

Frank, J. N. (1998). The campus card conundrum. *Card Technology*, 25-31.

FSUCard Services (1996) *Use your SmartWorld chip today.* http://www.fsucard.fsu.edu/svc2.htm/ Last modified May 10, 1996. Accessed December 15, 1998. Email: ccorum@garnet.acns.fsu.edu

FSUCard Services (1999) *The FSUCard.* http://www.fsucard.fsu.edu Last modified January 22, 1999. Accessed June 13, 1999.

Gemplus smart card driver's license in Argentina. (1999). http://www.cardshow.com.guide/card/gemplus.html Last modified May 5, 1999. Accessed May 31, 1999. Email: webmaster@cardshow.com

Global ChipCard Alliance (1999). *About the Global ChipCard Alliance.* http://www.chipcard.org/about/introduction/content.html Last modified April 9, 1999. Accessed June 1, 1999.

Global ChipCard Alliance (1998). *The future of smart card technology worldwide.* http://www.chipcard.org Last modified October 6, 1998. Accessed May 30, 1999.

Gold, S. (1998, July 30). Bank of America plans Internet loadable Visa Cash. *Newsbytes,* 151.

Groenfeldt, T. (1997, March). Taking the e-commerce challenge. *Bank Systems & Technology,* 34 (3), 30-35.

GSM Association (1998). *History of GSM.* http://www.gsmworld.com/history/index.htm Last modified February 16, 1998. Accessed May 30, 1999.

Guthery, S. B. & Jurgensen, T. M. (1998). *Smart Card developer's kit.* Indianapolis, IN: Macmillian Technical Publishing.

Hale, J. L. (1999, February). Putting together the pieces. *American School and University,* 71 (6), 42-45.

Health Card Technologies, Inc. (1997). *Answers to frequently asked questions about medical smart cards.* http://hct.com/faq.htm Last modified September 29, 1997. Accessed June 7, 1999.

Health Passport (1998). *Health Passport: A project of the Western Governor's Association - frequently asked questions.* http://www.westgov.org/hpp/hpp_web.htm Last modified February 14, 1998. Accessed June 7, 1999.

Hofland, P. & Janowski, L. (1998, February). Better processor and memory technologies, open APIs, and new Oses pave the way for multiple applications running on one smartcard. *BYTE,* 24 (2), 55+.

Hyundai Semiconductor Group (1998). *What is FeRAM?* http://kcs.hei.co.kr/models/fram/fram.html Last modified December 22, 1998. Accessed June 2, 1999.

ID2tech (1999). *PKI smart cards.* http://www.id2tech.com Accessed December 21, 1999.

Information Society Technologies (1999, December 15). *Telematics for libraries: The TOLIMAC Project.* http://www.ech.lu/libraries

Infowin (1999). SCARAB: *Smart card and agent enabled reliable access.* http://www.infowin.org/ACTS/RUS/PROJECTS/ac339.htm Accessed December 21, 1999.

Iowa State University (1999). *ISU Card anatomy.* http://www.adp.iastate.edu/idcard/index.html Accessed June 13, 1999.

Jackson, W. (1999, April 12). VA tests medical smart cards. *Government Computer News.* http://www.gcn.com/gcn/1999/April12/34.htm Last modified April 13, 1999. Accessed June 7, 1999.

Java Card Platform (1999). *Java Card.* http://www.interl.net/~njohnson/thejava.htm Last modified April 19, 1999. Accessed July 31, 1999.

Kaplan, K. (1998, October 11). E-commerce may help Americans learn to love smart cards; technology: some believe the Net will give the chip-embedded plastic the acceptance it's long had in Europe. *The Los Angeles Times.*

Keenan, W., Rea, M. & Hubbard, G. (1997). Leveraging new business opportunities and differentiating your products and services. In C. A. Allen & W. J. Barr (Eds.), *Smart cards: Seizing strategic business opportunities* (pp. 79-89). Chicago, IL: Richard D. Irwin.

Kessler, G. & Sheppard, S. (1997, August). Time to spend electronic money. *Network VAR,* 5 (8), 65-72.

Klie, L. (1999, April). Bank deal expands card us on, off campus. *On-Campus Hospitality,* (21) 3, 20-22.

Kosiur, D. (1997, May 5). Smart Cards: Living up to potential? *PC Week,*14 (18), 105.

Krueger, J. & Schloss, R. (1998, September 9). *Recent reports have focused world attention on card security.* http://www.smartcrd.com/news/policy/security.htm Accessed December 21, 1999

Lemos, R. (1997, April 4). *Java gets smart (cards).* http://www5.zdnet.com/zdnn/content/pcwo/0404/pcwo0013.html Last modified April 19, 1999. Accessed May 30, 1999.

Leung, A. (1999, March 8). Tech spotlight: Smart cards seem a sure bet. *InfoWorld,* 21 (10), 37.

MacLellan, A. (1997, March 24). Motorola forms smartcard unit. *Electronic News*, 43 (21), 1.

Maki, D. A. (1999). Industry suppliers believe in the system. *Card Technology,* 48-50+.

Massachusetts Institute of Technology (1998) *The MIT Card* http://web.mit.edu/mitcard Last modified March 13, 1998. Accessed June 13, 1999.

MasterCard International (1999). *Smart cards and electronic commerce: a sure bet for the banks.* http://www.mastercard.com/ourcards/smartcard/articles/article3.html Accessed June 22, 1999.

MasterCard International (1999). *Frequently asked questions.* http://www.mastercard.com/ourcards/smartcard/ Assessed June 22, 1999.

MasterCard International (1999). *Japanese MYCAL program on track for five million.* http://www.mastercard.com/about/press/990511b.html Last modified May 11, 1999. Accessed June 22, 1999.

Medical smart cards. (1998). *Medical smart cards.* http://www.slv.ac.uk/~c9462782/medicalsc.htm Last modified June 1, 1998. Accessed June 7, 1999.

McGraw, G. & Felten, E. (1999). *Securing JAVA: Getting down to business with mobile code.* http://www.securingjava.com Last modified April 18, 1999. Accessed May 30, 1999.

Microsoft (1998, October 27). *Microsoft enters the smart card market with low-cost, easy-to-use approach.* http://www.microsoft.com/PressPass/features/1998/10-27smartcard.htm Last modified October 27, 1998. Accessed June 5, 1999.

Microsoft (1999). *Smart Card for Windows - The smart card market opportunity.* http://www.microsoft.com/PressPass/FEATURES/1998/SMARTCARDBG.HTM Last modified June 2, 1999. Accessed June 5, 1999.

Microsoft (1999). *Momentum builds for Smart Card for Windows.* http://www.microsoft.com/PressPass/PRESS/1999/MAY99/CTSTPR.HTM Last modified June 2, 1999. Accessed June 5, 1999.

Microsoft (1999). *Smart Card for Windows industry support.* http://agent.microsoft.com/windowsce/smartcard/start/ind-sup.asp Last modified May 10, 1999. Accessed June 5, 1999.

Miller, B. (1993, September/October). A smart approach to security. *Infosecurity News,* 4 (5), 27-28.

Mitchell, R. (1999, April 1). A ringing mobile phone success – the use of Subscriber Identification Module cards to support GSM cellular phones already is one of the smart card industry's strongest markets. But with chip cards being positioned to support a wide range of phone applications, the smart card is helping to transform the handset into a wireless computer and access device. *Card Technology,* N/A.

M'Soft preps entry into smart cards. (1999, May 17). *Electronic Engineering Times,* 8.

Mondex (1999). *How Mondex works.* http://www.mondexusa.com/html/content/technolo/technolo.htm#transact Accessed December 21, 1999.

Multos (1997, November 3). *Multos Homepage.* http://www.multos.com Last modified November 3, 1997. Accessed June 1, 1999.

Myhill, M. (1998, February). Smartcards in libraries: a brave new world. *The Electronic Library*, 16 (1), 17-23.

NACCU (1999). *The National Association of Campus Card Users.* http://www.naccu.org Last updated June 1, 1999. Accessed July 12, 1999.

NEC (1998). *NEC develops embedded FeRAM for smart card LSIs.* http://www.sunrise.co.uk/embedded_FeRAM.htm Last modified August 14, 1998. Accessed June 2, 1999.

Nelson, M. (1998, June 8). Smart cards: A work in progress. *InfoWorld,* 20 (23), 1.

Norusis, M. N. (1991). *SPSS/PC+ Studentware.* Chicago, IL: SPSS Inc.

Nottingham moves to the head of the campus card class (1998). *Smart Card Alert*, 2.

Nova Southeastern University Fact Book (1999). Nova Southeastern University Research and Planning Department.

Ognibene, P. J. (1996, May 29). *Smart Cards: The next generation for electronic toll collection.* http://www.ettm.com/news/etcsmart.html Last modified May 29, 1996. Accessed June 19, 1999.

One small step for smartcards. (1998, July 6). *Electronic News*, 44 (2226), 4.

O'Sullivan, O. (1999, March). Cash it ain't. *USBanker,* 109 (3), 42-51.

Overview of smart card technology (1999, June 14). http://www.bit-inc.com/htmlfiles/newsndx.htm Last modified June 14, 1999. Accessed July 26, 1999.

PC/SC Workgroup (1998) *PC/SC Workgroup releases first specifications for integration of smart cards with personal computers.* http://www.smartcardsys.com Last modified May 12, 1998. Accessed January 30, 1999. Email: pcsc@slb.com

PC/SC Workgroup (1996) *PC/SC Workgroup Overview.* http://www.smartcardsys.com/index.html Last modified December 9, 1996. Accesses May 30, 1999.

Phillips, S. (1998, August 20). Smartcards are just the ticket for Tube. Computer Weekly, 8.

Picado, R. (1998, February 12). *Electronic Toll Collection.* http://www.path.berkeley.edu/~leap/EP/Electronic_Payment/electron_toll.html Last modified February 12, 1998. Accessed June 15, 1999.

Printup, R. (1997, May). Magnetic Stripes at Stanford - A solid business case still needed for smart cards. *Cardtech Securtech - Conference Proceedings - 1997.* (2), 55-66.

Rigney, M. (1998, November). More schools stateside, abroad get smarter about campus card programs. *Card Marketing,* 2 (10), 6.

Ruscitti, G., Fabrizi, E., Aleggianai, F. & Nasi, M. (1997, November). CARDLINK: A European project for the implementation of an interoperable emergency dataset on a smart card. The Rome pilot site experience. *Studies in Health Technology and Informatics*, 49, 289-291.

Schneier, B. & Shostack, A. (1999, November 19). *Breaking up is hard to do: modeling security threats for smart cards.* http://www.counterpaine.com/smart-card-threats.html

Schlumberger (1999). *Schlumberger announces first Windows 2000-compatible smart card for network security.* http://www.slb.com/ir/news/sct-interop9903.html Last modified March 29, 1999. Accessed June 5, 1999.

Sharpe, B. & Warthen, M. (1997, November). The case for smart cards in the U.S. healthcare industry. *Studies in Health Technology and Informatics*, 49, 355-360.

Simms, M. (1999, January). Merrill, Microsoft seek security in smart cards. *Wall Street & Technology,*(17) 1, 22.

SJB Research (1999). *The Smart Card.* http://www.sjbresearch.com/tsc.html Last modified June 1, 1999. Accessed June 15, 1999.

SJB Services (1998). *Multos.* http://www.tag.no/multos.htm Last modified December 8, 1998. Accessed July 31, 1999.

Smart cards fill a network safety need. (1999, March). *Smart Card Alert,* 1.

SmartCard Club (1999). *About DISTINCT.* http://www.smartcardclud.co.uk/ Accessed December 21, 1999

Smart Card Forum (1998) *What is a Smart Card?* http://www.smartcardforum.org/news/whatis.htm Last modified September 1, 1998. Accessed May 7, 1999. Email: info@smartcardforum.org

Smart Card Forum (1999, February 3). *Smart Card Forum creates new membership category to reflect smart card success in education sector.* http://www.smartcardforum.org/news/press/EducationCategory.htm Last modified February 3, 1999. Accessed March 21, 1999. Email: info@smartcardforum.org

Smart Card Forum (1999, September 22). *Emphasis on Internet ID and Authentication Central to the Smart Card Forum Strategic Direction for 2000.* http://www.smartcrd.com/news/press/pkiworkgroup.htm Accessed December 21, 1999.

Smart Card Industry Association (1998). *About smart cards: smart card standards.* http://www.scia/org/aboutsc/stand.html Accessed July 17, 1999.

Smart Commerce Japan (1998). *What is SCJ?* http://www.scj.or.jp/scj_e.html Last modified July 17, 1998. Accessed June 12, 1999.

Smith, M., Cunningham, D. & Cunningham, D. (1997). Education. In C. A. Allen & W. J. Barr (Eds.), *Smart cards: Seizing strategic business opportunities* (pp. 224-233). Chicago, IL: Richard D. Irwin.

Souped-up SIM cards turn mobile phones into mini-computers (1999, April). *Smart Card Alert,* 1.

Symetrix Corporation (1998). *RFID smart cards.* http://www.symetrixcorp.com/Products1.html Last modified June 4, 1998. Accessed June 2, 1999.

Taaffe, J. & Johnston, M. (1997, July 22). *Siemens licenses Java for smart cards: smart card market expected to grow wildly, according to company.* http://www.javaworld.com/jw-08-1997/jw-08-idgns.smartcards.html Last modified April 8, 1999. Accessed May 30, 1999.

The Saturn Project (2000, January). *Smart cards: interfaces for people with disabilities.* http://www.trace.wisc.edu/docs/smartcards/schome.htm

Thomasson, J. P. & Baldi, L. (1997). Smartcards: portable security. *Annual IEEE International Conference on Innovative Systems in Silicon* (pp. 259-265). IEEE Computer Society Press.

Thomson, S. C. (1999, March 11). Washington U says smart cards aren't used enough. *St. Louis Post Dispatch*, B2.

Tobin, A. (1998). Only visionaries need apply. *Card Technology,* 22-26.

Tom, R. & Driver, J. (1998, September 19). *Smart cards technology report.* http://theweb.badm.sc.edu/701fstu/tom/smrtcrd.htm Last modified September 19, 1998. Accessed July 24, 1999.

Townend, R. C. (1999). *Finance: History, development and market overview.* http://www.smartcard.co.uk/finance1.html Accessed March 20, 1999. Email: scn@pavilion.co.uk

Towson University (1998). *Borrowing materials.* http://www.towson.edu Last modified April 12, 1998. Accessed June 13, 1999.

University of Edinburgh (1999). *The university smart card project.* http://www.admin.ed.ac.uk/smartcard/index.htm Last modified February 4, 1999. Accessed August 8, 1999.

University of Michigan (1999). *MCard overview.* http://www.mcard.umich.edu/cashchip.htm Last modified March 2, 1999. Accessed June 13, 1999.

University of Toledo (1999). *The University of Toledo ID Center/Campus Card Office.* http://saserv.utoledo.edu/id-center/index.html Last modified March 15, 1999. Accessed June 13, 1999.

Villanova University (1998). *Wildcard Homepage.* http://dgprod2.will.edu/admin/wildcard/homepage.htm Last modified September 15, 1998. Accessed December 15, 1998.

Visa International (1999). *Visa Cash on the Internet.* http://www.visa.com/nt/chip/vcashint.html Accessed June 12, 1999.

Visa (1999). *Visa Cash in Celebration, Florida.* http://www.visa.com/nt/cash/celebration.html Last modified April 14, 1999. Accessed June 12, 1999.

Visa (1999, April 8). New Visa Cash service to provide 'anytime, anywhere' access to electronic cash. http://www.boot.co.za/news/april99/smartcard8.htm Last modified April 16, 1999. Accessed June 12, 1999.

Visa SET Protocol (1999). *Frequently asked questions about SET.* http://www-s2.visa.com.au/nt/abt_set/faq.html Accessed December 21, 1999.

Visa Smart Card Specs-EMV (1999, April 14). *EMV integrated circuit card specifications.* http://www.visa.com/nt/chip/history.html Last modified April 14, 1999. Accessed August 2, 1999.

Wand, S. & Thermos, A. C. (1998, June). Gaining access. *American School & University*, 70 (10), 34+.

Washington University in St. Louis (1998) *Campus CacheCard.* http://cf6000.wustl.edu/~regis/ids.htm Last modified September 1, 1998. Accessed December 12, 1998. Email: p71400ro@wuvmd.wustl.edu

Watson, T. (1997, September 5). Chipcards need standards to get smarter. *Computing Canada*, 23 (19), 18.

Wells Fargo (1998, September 5). *Wells Fargo takes giant leap in electronic commerce with new smart card pilot on the Internet.* http://wellsfargo.com/press/press980915/ Last modified April 16, 1999. Accessed June 22, 1999.

White, L. (1998). Full house. *American School & University*, 71.

Whitten, J. L., Bentley, L. D. & Barlow, B. M. (1994). *Systems analysis & design* (3rd ed.). Boston, MA: Richard D. Irwin, Inc.

Wilen, J. (1997, April 7). Penn envisions a safer campus where smart cards replace cash. *Philadelphia Business Journal.* http://www.amcity.com/philadelphia/stories/040797/focus6.html Last modified October 16, 1998. Accessed July 17, 1999.

Woods, K. (1989, May 1). Card smarts: Wallet sized computers. *PC/Computing*, 2 (5), 169-170.

World Standards Services Network (1998, November 3). *General Info on Standardizations.* http://www.wssn.net/WSSN/gen_inf.htm Last modified November 3, 1998. Accessed July 17, 1999.

Yin, R. K. (1994). *Case Study Research: Design and Methods* (2nd ed.). Thousand Oaks, CA: SAGE Publications.

Zoreda, J. L. & Oton, J. M. (1994). *Smart cards.* Norwood, MA: Artech House, Inc.